**微软发布3月补丁修复75个安全问题**

**安全威胁通告**



发布时间：2018年3月14日

## 综述

微软于周二发布了3月安全更新补丁，修复了75个从简单的欺骗攻击到远程执行代码的安全问题，产品涉及.NET Core、Adobe Flash Player、ASP .NET、ASP.NET、Device Guard、Internet Explorer、Microsoft Browsers、Microsoft Edge、Microsoft Exchange Server、Microsoft Graphics Component、Microsoft Office、Microsoft Scripting Engine、Microsoft Video Control、Microsoft Windows、Windows Desktop Bridge、Windows Hyper-V、Windows Installer、Windows Kernel以及Windows Shell。

相关信息如下（红色部分威胁相对比较高）：

|  |  |  |
| --- | --- | --- |
| 产品 | CVE 编号 | CVE 标题 |
| .NET Core | CVE-2018-0875 | .NET Core 拒绝服务漏洞 |
| Adobe Flash Player | ADV180006 | March 2018 Adobe Flash 安全更新 |
| ASP .NET | CVE-2018-0787 | ASP.NET Core 特权提升漏洞 |
| ASP.NET | CVE-2018-0808 | ASP.NET Core 拒绝服务漏洞 |
| Device Guard | CVE-2018-0884 | Windows 安全功能绕过漏洞 |
| Internet Explorer | CVE-2018-0929 | Internet Explorer 信息泄露漏洞 |
| Internet Explorer | CVE-2018-0942 | Internet Explorer 特权提升漏洞 |
| Microsoft Browsers | CVE-2018-0927 | Microsoft Browser 信息泄露漏洞 |
| Microsoft Browsers | CVE-2018-0932 | Microsoft Browser 信息泄露漏洞 |
| Microsoft Edge | CVE-2018-0879 | Microsoft Edge 信息泄露漏洞 |
| Microsoft Exchange Server | CVE-2018-0924 | Microsoft Exchange 信息泄露漏洞 |
| Microsoft Exchange Server | CVE-2018-0940 | Microsoft Exchange 特权提升漏洞 |
| Microsoft Exchange Server | CVE-2018-0941 | Microsoft Exchange 信息泄露漏洞 |
| Microsoft Graphics Component | CVE-2018-0816 | Windows GDI 特权提升漏洞 |
| Microsoft Graphics Component | CVE-2018-0817 | Windows GDI 特权提升漏洞 |
| Microsoft Graphics Component | CVE-2018-0815 | Windows GDI 特权提升漏洞 |
| Microsoft Office | CVE-2018-0947 | Microsoft Sharepoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-0903 | Microsoft Access 远程代码执行漏洞 |
| Microsoft Office | CVE-2018-0909 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-0910 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-0907 | Microsoft Office Excel Security Feature Bypass |
| Microsoft Office | CVE-2018-0911 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-0912 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-0913 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-0914 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-0915 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-0916 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-0917 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-0919 | Microsoft Office 信息泄露漏洞 |
| Microsoft Office | CVE-2018-0921 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-0922 | Microsoft Office 内存破坏漏洞 |
| Microsoft Office | CVE-2018-0923 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2018-0944 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Scripting Engine | CVE-2018-0889 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0891 | Scripting Engine 信息泄露漏洞 |
| Microsoft Scripting Engine | CVE-2018-0893 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0930 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0931 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0933 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0934 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0935 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0936 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0937 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0939 | Scripting Engine 信息泄露漏洞 |
| Microsoft Scripting Engine | CVE-2018-0872 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0873 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0874 | Chakra Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0876 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2018-0925 | Scripting Engine 内存破坏漏洞 |
| Microsoft Video Control | CVE-2018-0881 | Microsoft Video Control 特权提升漏洞 |
| Microsoft Windows | CVE-2018-0886 | CredSSP 远程代码执行漏洞 |
| Microsoft Windows | CVE-2018-0902 | CNG 安全功能绕过漏洞 |
| Microsoft Windows | CVE-2018-0983 | Windows Storage Services 特权提升漏洞 |
| Microsoft Windows | CVE-2018-0878 | Windows Remote Assistance 信息泄露漏洞 |
| Windows Desktop Bridge | CVE-2018-0877 | Windows Desktop Bridge VFS 特权提升漏洞 |
| Windows Desktop Bridge | CVE-2018-0880 | Windows Desktop Bridge 特权提升漏洞 |
| Windows Desktop Bridge | CVE-2018-0882 | Windows Desktop Bridge 特权提升漏洞 |
| Windows Hyper-V | CVE-2018-0885 | Windows Hyper-V 拒绝服务漏洞 |
| Windows Hyper-V | CVE-2018-0888 | Hyper-V 信息泄露漏洞 |
| Windows Installer | CVE-2018-0868 | Windows Installer 特权提升漏洞 |
| Windows Kernel | CVE-2018-0811 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0894 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0895 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0896 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0897 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0898 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0899 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0900 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0901 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0926 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0977 | Win32k 特权提升漏洞 |
| Windows Kernel | CVE-2018-0813 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0814 | Windows Kernel 信息泄露漏洞 |
| Windows Kernel | CVE-2018-0904 | Windows Kernel 信息泄露漏洞 |
| Windows Shell | CVE-2018-0883 | Windows Shell 远程代码执行漏洞 |

## 修复建议

微软官方已经发布更新补丁，请及时进行补丁更新。

## 附件

# ADV180006 - March 2018 Adobe Flash Security Update

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| ADV180006 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=ADV180006) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=ADV180006) | **CVE Title:** March 2018 Adobe Flash Security Update  **Description:**  This security update addresses the following vulnerabilities, which are described in Adobe Security Bulletin [APSB18-05](http://helpx.adobe.com/security/products/flash-player/apsb18-05.html): CVE-2018-4919 and CVE-2018-4920.  **FAQ:**  **How could an attacker exploit these vulnerabilities?** In a web-based attack scenario where the user is using Internet Explorer for the desktop, an attacker could host a specially crafted website that is designed to exploit any of these vulnerabilities through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit any of these vulnerabilities. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by clicking a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email.  In a web-based attack scenario where the user is using Internet Explorer in the Windows 8-style UI, an attacker would first need to compromise a website already listed in the Compatibility View (CV) list. An attacker could then host a website that contains specially crafted Flash content designed to exploit any of these vulnerabilities through Internet Explorer and then convince a user to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by clicking a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email. For more information about Internet Explorer and the CV List, please see the MSDN Article, Developer Guidance for websites with content for Adobe Flash Player in Windows 8.  **Mitigations:**  **Workarounds:**  Workaround refers to a setting or configuration change that would help block known attack vectors before you apply the update.  **Prevent Adobe Flash Player from running** You can disable attempts to instantiate Adobe Flash Player in Internet Explorer and other applications that honor the kill bit feature, such as Office 2007 and Office 2010, by setting the kill bit for the control in the registry.  **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. To set the kill bit for the control in the registry, perform the following steps:   1. Paste the following into a text file and save it with the .reg file extension. 2. Windows Registry Editor Version 5.00 3. [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] 4. "Compatibility Flags"=dword:00000400 5. [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] 6. "Compatibility Flags"=dword:00000400 7. Double-click the .reg file to apply it to an individual system.   You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, Group Policy collection.  **Note** You must restart Internet Explorer for your changes to take effect. **Impact of workaround**. There is no impact as long as the object is not intended to be used in Internet Explorer. **How to undo the workaround.** Delete the registry keys that were added in implementing this workaround. **Prevent Adobe Flash Player from running in Internet Explorer through Group Policy** **Note** The Group Policy MMC snap-in can be used to set policy for a machine, for an organizational unit, or for an entire domain. For more information about Group Policy, visit the following Microsoft Web sites:  [Group Policy Overview](https://technet.microsoft.com/library/hh831791) [What is Group Policy Object Editor?](https://technet.microsoft.com/library/cc737816%28v=ws.10%29.aspx) [Core Group Policy tools and settings](https://technet.microsoft.com/library/cc784165%28v=ws.10%29.aspx)  To disable Adobe Flash Player in Internet Explorer through Group Policy, perform the following steps: **Note** This workaround does not prevent Flash from being invoked from other applications, such as Microsoft Office 2007 or Microsoft Office 2010.   1. Open the Group Policy Management Console and configure the console to work with the appropriate Group Policy object, such as local machine, OU, or domain GPO. 2. Navigate to the following node: **Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Add-on Management** 3. Double-click **Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects**. 4. Change the setting to Enabled. 5. Click **Apply** and then click **OK** to return to the Group Policy Management Console. 6. Refresh Group Policy on all systems or wait for the next scheduled Group Policy refresh interval for the settings to take effect. **Prevent Adobe Flash Player from running in Office 2010 on affected systems** **Note** This workaround does not prevent Adobe Flash Player from running in Internet Explorer. **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. For detailed steps that you can use to prevent a control from running in Internet Explorer, see Microsoft Knowledge Base Article 240797. Follow the steps in the article to create a Compatibility Flags value in the registry to prevent a COM object from being instantiated in Internet Explorer.   To disable Adobe Flash Player in Office 2010 only, set the kill bit for the ActiveX control for Adobe Flash Player in the registry using the following steps:   1. Create a text file named Disable\_Flash.reg with the following contents:   [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Office\Common\COM\Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}]  "Compatibility Flags"=dword:00000400   1. Double-click the .reg file to apply it to an individual system. 2. **Note** You must restart Internet Explorer for your changes to take effect. You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, [Group Policy collection](http://go.microsoft.com/fwlink/?LinkID=215719). **Prevent ActiveX controls from running in Office 2007 and Office 2010**   To disable all ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, including Adobe Flash Player in Internet Explorer, perform the following steps:   1. Click File, click Options, click Trust Center, and then click Trust Center Settings. 2. Click ActiveX Settings in the left-hand pane, and then select Disable all controls without notifications. 3. Click OK to save your settings. **Impact of workaround**. Office documents that use embedded ActiveX controls may not display as intended. **How to undo the workaround**.   To re-enable ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, perform the following steps:   1. Click File, click Options, click Trust Center, and then click Trust Center Settings. 2. Click ActiveX Settings in the left-hand pane, and then deselect Disable all controls without notifications. 3. Click OK to save your settings. **Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones** You can help protect against exploitation of these vulnerabilities by changing your settings for the Internet security zone to block ActiveX controls and Active Scripting. You can do this by setting your browser security to High.   To raise the browsing security level in Internet Explorer, perform the following steps:   1. On the Internet Explorer **Tools** menu, click\*\* Internet Option\*\*s. 2. In the **Internet Options** dialog box, click the **Security** tab, and then click **Internet**. 3. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 4. Click **Local intranet**. 5. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 6. Click **OK** to accept the changes and return to Internet Explorer. **Note** If no slider is visible, click **Default Level**, and then move the slider to **High**. **Note** Setting the level to High may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly even with the security setting set to High. **Impact of workaround**. There are side effects to blocking ActiveX Controls and Active Scripting. Many websites on the Internet or an intranet use ActiveX or Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX Controls to provide menus, ordering forms, or even account statements. Blocking ActiveX Controls or Active Scripting is a global setting that affects all Internet and intranet sites. If you do not want to block ActiveX Controls or Active Scripting for such sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". **Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone**   You can help protect against exploitation of these vulnerabilities by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone. To do this, perform the following steps:   1. In Internet Explorer, click **Internet Options** on the **Tools** menu. 2. Click the **Security** tab. 3. Click **Internet**, and then click **Custom Level**. 4. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 5. Click **Local intranet**, and then click **Custom Level**. 6. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 7. Click **OK** to return to Internet Explorer, and then click **OK** again. **Note** Disabling Active Scripting in the Internet and Local intranet security zones may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly. **Impact of workaround**. There are side effects to prompting before running Active Scripting. Many websites that are on the Internet or on an intranet use Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use Active Scripting to provide menus, ordering forms, or even account statements. Prompting before running Active Scripting is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you feel you trust the site that you are visiting, click **Yes** to run Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". **Add sites that you trust to the Internet Explorer Trusted sites zone** After you set Internet Explorer to require a prompt before it runs ActiveX controls and Active Scripting in the Internet zone and in the Local intranet zone, you can add sites that you trust to the Internet Explorer Trusted sites zone. This will allow you to continue to use trusted websites exactly as you do today, while helping to protect you from this attack on untrusted sites. We recommend that you add only sites that you trust to the Trusted sites zone.   To do this, perform the following steps:   1. In Internet Explorer, click **Tools**, click **Internet Options**, and then click the **Security** tab. 2. In the **Select a web content zone to specify its current security settings** box, click **Trusted Sites**, and then click **Sites**. 3. If you want to add sites that do not require an encrypted channel, click to clear the **Require server verification (https:) for all sites in this zone** check box. 4. In the **Add this website to the zone** box, type the URL of a site that you trust, and then click **Add**. 5. Repeat these steps for each site that you want to add to the zone. 6. Click **OK** two times to accept the changes and return to Internet Explorer. **Note** Add any sites that you trust not to take malicious action on your system. Two sites in particular that you may want to add are \***.windowsupdate.microsoft.com** and \***.update.microsoft.com**. These are the sites that will host the update, and they require an ActiveX control to install the update.   **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **ADV180006** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Adobe Flash Player on Windows Server 2012 | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 8.1 for 32-bit systems | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 8.1 for x64-based systems | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows Server 2012 R2 | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows RT 8.1 | 4088785 Security Update | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 for 32-bit Systems | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 for x64-based Systems | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1511 for x64-based Systems | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1511 for 32-bit Systems | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows Server 2016 | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1709 for 32-bit Systems | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1709 for x64-based Systems | [4088785 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088785) | Critical | Remote Code Execution | 4056887 | Base: N/A Temporal: N/A Vector: N/A | Yes |

# CVE-2018-0787 - ASP.NET Core Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0787 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0787) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0787) | **CVE Title:** ASP.NET Core Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when a Kestrel web application fails to validate web requests.  An attacker who successfully exploited this vulnerability could perform HTML injection attacks.  To exploit the vulnerability, an attacker could send a specially crafted request, containing injected HTML, to the web application. The specially crafted request would initiate a "password reset" email to the target user. Depending on the target user email client, the injected HTML could trigger as soon as the target user opens the "password reset" e-mail.  The security update addresses the vulnerability by correcting how a Kestrel web application validates web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0787** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| ASP.NET Core 2.0 | [Commit Security Update](https://github.com/aspnet/Announcements/issues/295) | Important | Elevation of Privilege |  | Base: N/A Temporal: N/A Vector: N/A | Yes |

# CVE-2018-0808 - ASP.NET Core Denial of Service Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0808 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0808) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0808) | **CVE Title:** ASP.NET Core Denial of Service Vulnerability  **Description:**  A denial of service vulnerability exists when ASP.NET Core improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against an ASP.NET Core web application. The vulnerability can be exploited remotely, without authentication.  A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the .NET Core application.  The update addresses the vulnerability by correcting how the ASP.NET Core web application handles web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Denial of Service |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0808** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| ASP.NET Core 2.0 | [Commit Security Update](https://github.com/aspnet/Announcements/issues/294) | Important | Denial of Service |  | Base: N/A Temporal: N/A Vector: N/A | Yes |

# CVE-2018-0811 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0811 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0811) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0811) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.  To exploit this vulnerability, an authenticated attacker could run a specially crafted application. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.  The update addresses the vulnerability by correcting how the Windows kernel initializes objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0811** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0813 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0813 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0813) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0813) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.  To exploit this vulnerability, an authenticated attacker could run a specially crafted application. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.  The update addresses the vulnerability by correcting how the Windows kernel initializes objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0813** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |

# CVE-2018-0814 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0814 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0814) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0814) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.  To exploit this vulnerability, an authenticated attacker could run a specially crafted application. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.  The update addresses the vulnerability by correcting how the Windows kernel initializes objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0814** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074598 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O | Yes |

# CVE-2018-0815 - Windows GDI Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0815 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0815) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0815) | **CVE Title:** Windows GDI Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.  The update addresses the vulnerability by correcting how GDI handles objects in memory and by preventing instances of unintended user-mode privilege elevation.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0815** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0816 - Windows GDI Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0816 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0816) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0816) | **CVE Title:** Windows GDI Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.  The update addresses the vulnerability by correcting how GDI handles objects in memory and by preventing instances of unintended user-mode privilege elevation.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0816** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Elevation of Privilege | 4074593 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Elevation of Privilege | 4074593 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Elevation of Privilege | 4074596 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Elevation of Privilege | 4074596 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Elevation of Privilege | 4074591 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Elevation of Privilege | 4074591 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0817 - Windows GDI Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0817 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0817) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0817) | **CVE Title:** Windows GDI Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.  The update addresses the vulnerability by correcting how GDI handles objects in memory and by preventing instances of unintended user-mode privilege elevation.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0817** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Elevation of Privilege | 4074593 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Elevation of Privilege | 4074593 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Elevation of Privilege | 4074596 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Elevation of Privilege | 4074596 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Elevation of Privilege | 4074591 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Elevation of Privilege | 4074591 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089344 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0868 - Windows Installer Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0868 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0868) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0868) | **CVE Title:** Windows Installer Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.  A locally authenticated attacker could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  The security update addresses the vulnerability by correcting the input sanitization error to preclude unintended elevation.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0868** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4087398 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4087398) | Important | Elevation of Privilege | 4074598 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Elevation of Privilege | 4074593 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Elevation of Privilege | 4074593 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Elevation of Privilege | 4074594 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Elevation of Privilege | 4074596 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Elevation of Privilege | 4074596 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Elevation of Privilege | 4074591 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Elevation of Privilege | 4074591 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4087398 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4087398) | Important | Elevation of Privilege | 4074588 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4087398 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4087398) | Important | Elevation of Privilege | 4074588 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4087398 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4087398) | Important | Elevation of Privilege | 4074588 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4087398 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4087398) | Important | Elevation of Privilege | 4074588 | Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0872 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0872 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0872) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0872) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0872** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Remote Code Execution | 4074596 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Remote Code Execution | 4074596 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Moderate | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Commit Security Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.2) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0873 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0873 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0873) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0873) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0873** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Low | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Commit Security Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.2) | Important | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0874 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0874 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0874) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0874) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0874** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Remote Code Execution | 4074596 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Remote Code Execution | 4074596 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Moderate | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Commit Security Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.2) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0875 - .NET Core Denial of Service Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0875 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0875) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0875) | **CVE Title:** .NET Core Denial of Service Vulnerability  **Description:**  A denial of service vulnerability exists in the way that .NET Core handles specially crafted requests, causing a hash collision.  To exploit the vulnerability, an attacker could send a small number of specially crafted requests to an .NET Core web application, causing performance to degrade significantly enough to cause a denial of service condition.  The security update addresses the vulnerability by correcting how .NET Core handles specially crafted requests to prevent a hash collision.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Denial of Service |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0875** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| .NET Core 1.0 | [Commit Security Update](https://github.com/dotnet/announcements/issues/62) | Important | Denial of Service |  | Base: N/A Temporal: N/A Vector: N/A | Yes |
| .NET Core 1.1 | [Commit Security Update](https://github.com/dotnet/announcements/issues/62) | Important | Denial of Service |  | Base: N/A Temporal: N/A Vector: N/A | Yes |
| .NET Core 2.0 | [Commit Security Update](https://github.com/dotnet/announcements/issues/62) | Important | Denial of Service |  | Base: N/A Temporal: N/A Vector: N/A | Yes |
| PowerShell Core 6.0.0 | [Release Notes Security Update](https://github.com/PowerShell/Announcements/issues) | Important | Denial of Service |  | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0876 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0876 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0876) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0876) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0876** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Remote Code Execution | 4074596 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Remote Code Execution | 4074596 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Moderate | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0877 - Windows Desktop Bridge VFS Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0877 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0877) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0877) | **CVE Title:** Windows Desktop Bridge VFS Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in Windows when the Desktop Bridge VFS does not take into acccount user/kernel mode when managing file paths. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.  The update addresses this vulnerability by correcting how the Windows Desktop Bridge VFS handles file path management.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0877** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |

# CVE-2018-0878 - Windows Remote Assistance Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0878 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0878) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0878) | **CVE Title:** Windows Remote Assistance Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Windows Remote Assistance incorrectly processes XML External Entities (XXE). An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.  To exploit this condition, an attacker would need to send a specially crafted Remote Assistance invitation file to a user. A attacker could then steal text files from known locations on the victim's machine, under the context of the user, or alternatively, steal text information from URLs accessible to the victim. The stolen information could be submitted as part of the URL in HTTP request(s) to the attacker. In all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action.  Note that the information disclosure vulnerability by itself would not be sufficient for an attacker to compromise a system. However, an attacker could combine this vulnerability with additional vulnerabilities to further exploit the system.  The update addresses the vulnerability by correcting how Windows Remote Assistance processes XML External Entities (XXE).  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0878** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089453 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074598 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089453 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089453 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089453 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089344) | Important | Information Disclosure | 4074588 | Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0879 - Microsoft Edge Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0879 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0879) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0879) | **CVE Title:** Microsoft Edge Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.  To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site.  The update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0879** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O | Yes |

# CVE-2018-0880 - Windows Desktop Bridge Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0880 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0880) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0880) | **CVE Title:** Windows Desktop Bridge Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in Windows when Desktop Bridge does not properly manage the virtual registry. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.  The update addresses this vulnerability by correcting how the Windows Desktop Bridge manages the virtual registry.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0880** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |

# CVE-2018-0881 - Microsoft Video Control Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0881 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0881) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0881) | **CVE Title:** Microsoft Video Control Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in Windows when the Microsoft Video Control mishandles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in system mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.  The update addresses this vulnerability by correcting how the Microsoft Video Control handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0881** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Elevation of Privilege | 4074598 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Elevation of Privilege | 4074593 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Elevation of Privilege | 4074593 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Elevation of Privilege | 4074594 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Elevation of Privilege | 4074596 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Elevation of Privilege | 4074596 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Elevation of Privilege | 4074591 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Elevation of Privilege | 4074591 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C | Yes |

# CVE-2018-0882 - Windows Desktop Bridge Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0882 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0882) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0882) | **CVE Title:** Windows Desktop Bridge Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in Windows when Desktop Bridge does not properly manage the virtual registry. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.  The update addresses this vulnerability by correcting how the Windows Desktop Bridge manages the virtual registry.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0882** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O | Yes |

# CVE-2018-0883 - Windows Shell Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0883 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0883) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0883) | **CVE Title:** Windows Shell Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists when Windows Shell does not properly validate file copy destinations.  An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.  To exploit the vulnerability, a user must open a specially crafted file. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and then convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force a user to visit the website. Instead, an attacker would have to convince a user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file.  The security update addresses the vulnerability by helping to ensure that Windows Shell validates file copy destinations.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0883** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Remote Code Execution | 4074598 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Remote Code Execution | 4074598 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Remote Code Execution | 4074598 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Remote Code Execution | 4074598 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Remote Code Execution | 4074598 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089175 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089175) | Important | Remote Code Execution | 4074598 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Remote Code Execution | 4074593 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Remote Code Execution | 4074593 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Remote Code Execution | 4074594 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Remote Code Execution | 4074594 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Remote Code Execution | 4074594 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Remote Code Execution | 4074594 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Remote Code Execution | 4074594 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Remote Code Execution | 4074596 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Remote Code Execution | 4074596 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Remote Code Execution | 4074591 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Remote Code Execution | 4074591 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Remote Code Execution | 4074590 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Remote Code Execution | 4074590 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Remote Code Execution | 4074590 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Remote Code Execution | 4074590 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Remote Code Execution | 4074592 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Remote Code Execution | 4074592 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Remote Code Execution | 4074588 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Remote Code Execution | 4074588 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089175 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089175) | Important | Remote Code Execution | 4074588 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089175 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089175) | Important | Remote Code Execution | 4074588 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089175 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089175) | Important | Remote Code Execution | 4074588 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089175 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089175) | Important | Remote Code Execution | 4074588 | Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |

# CVE-2018-0884 - Windows Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0884 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0884) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0884) | **CVE Title:** Windows Security Feature Bypass Vulnerability  **Description:**  A security feature bypass vulnerability exists in Windows Scripting Host which could allow an attacker to bypass Device Guard. An attacker who successfully exploited this vulnerability could circumvent a User Mode Code Integrity (UMCI) policy on the machine.  To exploit the vulnerability, an attacker would first have to access the local machine, and then run a malicious program.  The update addresses the vulnerability by correcting how Windows Scripting Host handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0884** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Security Feature Bypass | 4074596 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Security Feature Bypass | 4074596 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Security Feature Bypass | 4074591 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Security Feature Bypass | 4074591 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Security Feature Bypass | 4074590 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Security Feature Bypass | 4074590 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Security Feature Bypass | 4074590 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Security Feature Bypass | 4074590 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Security Feature Bypass | 4074592 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Security Feature Bypass | 4074592 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Security Feature Bypass | 4074588 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Security Feature Bypass | 4074588 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Security Feature Bypass | 4074588 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |

# CVE-2018-0885 - Windows Hyper-V Denial of Service Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0885 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0885) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0885) | **CVE Title:** Windows Hyper-V Denial of Service Vulnerability  **Description:**  A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. An attacker who successfully exploited the vulnerability could cause the host server to crash.  To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash.  The update addresses the vulnerability by modifying how virtual machines access the Hyper-V Network Switch.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Denial of Service |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0885** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Denial of Service | 4074598 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Denial of Service | 4074598 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Denial of Service | 4074593 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Denial of Service | 4074593 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Denial of Service | 4074594 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Denial of Service | 4074594 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Denial of Service | 4074594 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Denial of Service | 4074594 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Denial of Service | 4074596 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Denial of Service | 4074591 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Denial of Service | 4074590 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Denial of Service | 4074590 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Denial of Service | 4074590 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Denial of Service | 4074592 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Denial of Service | 4074588 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Denial of Service | 4074588 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4073011 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4073011) | Important | Denial of Service | 4074588 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4073011 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4073011) | Important | Denial of Service | 4074588 | Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0886 - CredSSP Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0886 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0886) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0886) | **CVE Title:** CredSSP Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists in the Credential Security Support Provider protocol (CredSSP). An attacker who successfully exploited this vulnerability could relay user credentials and use them to execute code on the target system.  CredSSP is an authentication provider which processes authentication requests for other applications; any application which depends on CredSSP for authentication may be vulnerable to this type of attack.  As an example of how an attacker would exploit this vulnerability against Remote Desktop Protocol, the attacker would need to run a specially crafted application and perform a man-in-the-middle attack against a Remote Desktop Protocol session. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  The security update addresses the vulnerability by correcting how Credential Security Support Provider protocol (CredSSP) validates requests during the authentication process.  To be fully protected against this vulnerability users must enable Group Policy settings on their systems and update their Remote Desktop clients. The Group Policy settings are disabled by default to prevent connectivity problems and users must follow the instructions documented [HERE](https://go.microsoft.com/fwlink/?linkid=866660) to be fully protected.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0886** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Remote Code Execution | 4074598 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Remote Code Execution | 4074598 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Remote Code Execution | 4074598 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Remote Code Execution | 4074598 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Remote Code Execution | 4074598 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4056564 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056564) | Important | Remote Code Execution | 4074598 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Remote Code Execution | 4074593 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Remote Code Execution | 4074593 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Remote Code Execution | 4074594 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Remote Code Execution | 4074594 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Remote Code Execution | 4074594 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Remote Code Execution | 4074594 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Remote Code Execution | 4074594 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Remote Code Execution | 4074596 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Remote Code Execution | 4074596 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Remote Code Execution | 4074591 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Remote Code Execution | 4074591 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Remote Code Execution | 4074590 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Remote Code Execution | 4074590 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Remote Code Execution | 4074590 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Remote Code Execution | 4074590 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Remote Code Execution | 4074592 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Remote Code Execution | 4074592 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Remote Code Execution | 4074588 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Remote Code Execution | 4074588 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Remote Code Execution | 4074588 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4056564 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056564) | Important | Remote Code Execution | 4074588 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4056564 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056564) | Important | Remote Code Execution | 4074588 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4056564 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056564) | Important | Remote Code Execution | 4074588 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4056564 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4056564) | Important | Remote Code Execution | 4074588 | Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0888 - Hyper-V Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0888 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0888) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0888) | **CVE Title:** Hyper-V Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker on a guest operating system could run a specially crafted application that could cause the Hyper-V host operating system to disclose memory information.  An attacker who successfully exploited the vulnerability could gain access to information on the Hyper-V host operating system.  The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0888** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4088827 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088827) | Important | Information Disclosure | 4074588 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4088827 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088827) | Important | Information Disclosure | 4074588 | Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0889 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0889 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0889) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0889) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Moderate | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0889** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Moderate | Remote Code Execution | 4074736 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Moderate | Remote Code Execution | 4074736 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Critical | Remote Code Execution | 4074736 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Critical | Remote Code Execution | 4074736 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Moderate | Remote Code Execution | 4074736 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Critical | Remote Code Execution | 4074594 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Critical | Remote Code Execution | 4074594 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Moderate | Remote Code Execution | 4074594 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows RT 8.1 | 4088876 Monthly Rollup | Critical | Remote Code Execution | 4074594 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Remote Code Execution | 4074596 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Remote Code Execution | 4074596 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Moderate | Remote Code Execution | 4074590 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 10 on Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Moderate | Remote Code Execution | 4074736 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0891 - Scripting Engine Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0891 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0891) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0891) | **CVE Title:** Scripting Engine Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft browsers. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.  In a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site.  The security update addresses the vulnerability by changing how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0891** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Information Disclosure | 4074736 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Information Disclosure | 4074736 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Important | Information Disclosure | 4074736 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Important | Information Disclosure | 4074736 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Information Disclosure | 4074736 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Important | Information Disclosure | 4074594 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Important | Information Disclosure | 4074594 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Low | Information Disclosure | 4074594 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Low | Information Disclosure | 4074590 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 10 on Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Information Disclosure | 4074736 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Low | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Commit Security Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.2) | Important | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0893 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0893 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0893) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0893) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0893** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Moderate | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0894 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0894 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0894) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0894) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0894** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0895 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0895 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0895) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0895) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0895** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0896 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0896 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0896) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0896) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0896** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0897 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0897 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0897) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0897) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0897** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0898 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0898 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0898) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0898) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0898** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0899 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0899 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0899) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0899) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0899** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0900 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0900 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0900) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0900) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0900** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0901 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0901 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0901) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0901) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0901** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0902 - CNG Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0902 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0902) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0902) | **CVE Title:** CNG Security Feature Bypass Vulnerability  **Description:**  A security feature bypass vulnerability exists in the Cryptography Next Generation (CNG) kernel-mode driver (cng.sys) when it fails to properly validate and enforce impersonation levels.  An attacker could exploit this vulnerability by convincing a user to run a specially crafted application that is designed to cause CNG to improperly validate impersonation levels, potentially allowing the attacker to gain access to information beyond the access level of the local user.  The security update addresses the vulnerability by correcting how the kernel-mode driver validates and enforces impersonation levels.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0902** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Security Feature Bypass | 4074596 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Security Feature Bypass | 4074596 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Security Feature Bypass | 4074591 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Security Feature Bypass | 4074591 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Security Feature Bypass | 4074590 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Security Feature Bypass | 4074590 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Security Feature Bypass | 4074590 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Security Feature Bypass | 4074590 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Security Feature Bypass | 4074592 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Security Feature Bypass | 4074592 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Security Feature Bypass | 4074588 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Security Feature Bypass | 4074588 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Security Feature Bypass | 4074588 | Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C | Yes |

# CVE-2018-0903 - Microsoft Access Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0903 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0903) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0903) | **CVE Title:** Microsoft Access Remote Code Execution Vulnerability  **Description:**  A remote code execution vulnerability exists in Microsoft Access software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.  Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Access. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file.  The security update addresses the vulnerability by correcting how Microsoft Access handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0903** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Access 2010 Service Pack 2 (32-bit editions) | [3114416 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=ec7091f9-fd55-4cf0-8c31-8571cf365610) | Important | Remote Code Execution | 3101544 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Access 2010 Service Pack 2 (64-bit editions) | [3114416 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=fd28885b-b452-4398-9fe4-a2bfc995468a) | Important | Remote Code Execution | 3101544 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Access 2016 (32-bit edition) | [4011665 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c8f5ec75-146f-44a9-95f1-cecc30775d1f) | Important | Remote Code Execution | 2910978 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Access 2016 (64-bit edition) | [4011665 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=99e88664-bd68-4dcb-a7dd-23202b5c08e0) | Important | Remote Code Execution | 2910978 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Access 2013 Service Pack 1 (32-bit editions) | [4011234 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=bbaea32f-e5ba-4ba9-906c-144d3145fd65) | Important | Remote Code Execution | 3085584 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Access 2013 Service Pack 1 (64-bit editions) | [4011234 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=d18d5d53-0349-447f-86d2-e445a7e46159) | Important | Remote Code Execution | 3085584 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions | Click to Run Security Update | Important | Remote Code Execution | 3085584 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution | 3085584 | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2018-0904 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0904 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0904) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0904) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a [Kernel Address Space Layout Randomization (ASLR)](https://technet.microsoft.com/en-us/library/security/dn848375.aspx#ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.  To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.  The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0904** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 7 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088878 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088878) [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074598 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4088880 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088880) | Important | Information Disclosure | 4074593 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) [4088879 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088879) | Important | Information Disclosure | 4074594 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4089229 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089229) | Important | Information Disclosure | 4074588 | Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0907 - Microsoft Office Excel Security Feature Bypass

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0907 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0907) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0907) | **CVE Title:** Microsoft Office Excel Security Feature Bypass  **Description:**  A security feature bypass vulnerability exists in Microsoft Office software by not enforcing macro settings on an Excel document. The security feature bypass by itself does not allow arbitrary code execution. To successfully exploit the vulnerability, an attacker would have to embed a control in an Excel worksheet that specifies a macro should be run. Â  To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted file with an affected version of Microsoft Office software. Â  The security update addresses the vulnerability by enforcing macro settings on Excel documents.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Security Feature Bypass |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0907** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Excel 2007 Service Pack 3 | [4011714 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=6fd1a1ce-868c-4d96-a874-a7b02a44b6fd) | Important | Security Feature Bypass | 4011602 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2010 Service Pack 2 (32-bit editions) | [4011675 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=51cd9d55-2a63-4737-a3a6-49b9718ab449) | Important | Security Feature Bypass | 4011660 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2010 Service Pack 2 (64-bit editions) | [4011675 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=b92ad577-003e-4e33-adb6-6d77a9670fed) | Important | Security Feature Bypass | 4011660 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (32-bit editions) | [4018291 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=df1de53d-ea3d-4ccc-97ed-4ea1bd51e749) | Important | Security Feature Bypass | 4011639 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 Service Pack 1 (64-bit editions) | [4018291 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=d945927e-1a32-4dc1-b6c4-2b8cedcc5324) | Important | Security Feature Bypass | 4011639 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2013 RT Service Pack 1 | 4018291 Security Update | Important | Security Feature Bypass | 4011639 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 for Mac | [Release Notes Security Update](https://go.microsoft.com/fwlink/p/?linkid=831049) | Important | Security Feature Bypass | 4011639 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Excel 2016 (32-bit edition) | [4011727 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=ff04867f-af92-4290-92b2-043681279bb1) | Important | Security Feature Bypass | 4011627 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Excel 2016 (64-bit edition) | [4011727 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=228118a7-c93e-4128-afa0-b80afa0ffb98) | Important | Security Feature Bypass | 4011627 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions | Click to Run Security Update | Important | Security Feature Bypass | 4011627 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions | Click to Run Security Update | Important | Security Feature Bypass | 4011627 | Base: N/A Temporal: N/A Vector: N/A | No |

# CVE-2018-0909 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0909 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0909) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0909) | **CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0909** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Project Server 2013 Service Pack 1 | [4018305 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=427b7f98-069b-4ee8-869d-2b9ed74a1ae0) | Important | Elevation of Privilege | 4011701 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4018293 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75313053-6472-451e-8623-d125975f6fe7) | Important | Elevation of Privilege | 4011680 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0910 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0910 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0910) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0910) | **CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0910** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Project Server 2013 Service Pack 1 | [4018305 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=427b7f98-069b-4ee8-869d-2b9ed74a1ae0) | Important | Elevation of Privilege | 4011701 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4018293 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75313053-6472-451e-8623-d125975f6fe7) | Important | Elevation of Privilege | 4011680 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0911 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0911 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0911) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0911) | **CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0911** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Project Server 2013 Service Pack 1 | [4018305 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=427b7f98-069b-4ee8-869d-2b9ed74a1ae0) | Important | Elevation of Privilege | 4011701 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4018293 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75313053-6472-451e-8623-d125975f6fe7) | Important | Elevation of Privilege | 4011680 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0912 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0912 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0912) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0912) | **CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0912** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Project Server 2013 Service Pack 1 | [4018305 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=427b7f98-069b-4ee8-869d-2b9ed74a1ae0) | Important | Elevation of Privilege | 4011701 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4018293 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75313053-6472-451e-8623-d125975f6fe7) | Important | Elevation of Privilege | 4011680 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0913 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0913 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0913) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0913) | **CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0913** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Project Server 2013 Service Pack 1 | [4018305 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=427b7f98-069b-4ee8-869d-2b9ed74a1ae0) | Important | Elevation of Privilege | 4011701 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4018293 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75313053-6472-451e-8623-d125975f6fe7) | Important | Elevation of Privilege | 4011680 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0914 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0914 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0914) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0914) | **CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0914** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Project Server 2013 Service Pack 1 | [4018305 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=427b7f98-069b-4ee8-869d-2b9ed74a1ae0) | Important | Elevation of Privilege | 4011701 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4018293 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75313053-6472-451e-8623-d125975f6fe7) | Important | Elevation of Privilege | 4011680 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0915 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0915 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0915) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0915) | **CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0915** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Project Server 2013 Service Pack 1 | [4018305 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=427b7f98-069b-4ee8-869d-2b9ed74a1ae0) | Important | Elevation of Privilege | 4011701 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4018293 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75313053-6472-451e-8623-d125975f6fe7) | Important | Elevation of Privilege | 4011680 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0916 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0916 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0916) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0916) | **CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0916** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Project Server 2013 Service Pack 1 | [4018305 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=427b7f98-069b-4ee8-869d-2b9ed74a1ae0) | Important | Elevation of Privilege | 4011701 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4018293 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75313053-6472-451e-8623-d125975f6fe7) | Important | Elevation of Privilege | 4011680 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0917 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0917 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0917) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0917) | **CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0917** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft SharePoint Enterprise Server 2016 | [4018293 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75313053-6472-451e-8623-d125975f6fe7) | Important | Elevation of Privilege | 4011680 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0919 - Microsoft Office Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0919 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0919) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0919) | **CVE Title:** Microsoft Office Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Microsoft Office software reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory. An attacker who successfully exploited the vulnerability could view out of bound memory.  Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software.  The security update addresses the vulnerability by properly initializing the affected variable.  **FAQ:**  **I have Microsoft Word 2010 installed. Why am I not being offered the 4011673 update?** The 4011673 update only applies to systems running specific configurations of Microsoft Office 2010. Some configurations will not be offered the update.  **I am being offered this update for software that is not specifically indicated as being affected in the Affected Software and Vulnerability Severity Ratings table. Why am I being offered this update?** When updates address vulnerable code that exists in a component that is shared between multiple Microsoft Office products or shared between multiple versions of the same Microsoft Office product, the update is considered to be applicable to all supported products and versions that contain the vulnerable component.  For example, when an update applies to Microsoft Office 2007 products, only Microsoft Office 2007 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2007, Microsoft Excel 2007, Microsoft Visio 2007, Microsoft Compatibility Pack, Microsoft Excel Viewer, or any other Microsoft Office 2007 product that is not specifically listed in the Affected Software table. Furthermore, when an update applies to Microsoft Office 2010 products, only Microsoft Office 2010 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2010, Microsoft Excel 2010, Microsoft Visio 2010, Microsoft Visio Viewer, or any other Microsoft Office 2010 product that is not specifically listed in the Affected Software table.  For more information on this behavior and recommended actions, see [Microsoft Knowledge Base Article 830335](https://support.microsoft.com/kb/830335). For a list of Microsoft Office products that an update may apply to, refer to the Microsoft Knowledge Base Article associated with the specific update.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0919** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft SharePoint Server 2010 Service Pack 2 | [4011705 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=d124096c-8545-42d8-87a3-c7929abfa6bb) | Important | Information Disclosure | 4011609 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2010 Service Pack 2 (32-bit editions) | [4011674 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=13ec5733-4eae-4e71-abe7-46c2bd292aa3) | Important | Information Disclosure | 4011659 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2010 Service Pack 2 (64-bit editions) | [4011674 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=0689f54e-5e2b-42df-9ee5-56b0c150461c) | Important | Information Disclosure | 4011659 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | [4011673 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=08f103c4-fa77-4156-af35-f89dca79bfbe) | Important | Information Disclosure | 4011658 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | [4011673 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=ad50d12b-f9b6-4870-bc94-5d83879c2081) | Important | Information Disclosure | 4011658 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office Web Apps 2010 Service Pack 2 | [4011709 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=f0bc5316-2a16-46fd-b2b8-23b237f8e662) | Important | Information Disclosure | 4011615 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2013 Service Pack 1 (32-bit editions) | [4011695 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=52c1a89e-7d46-462d-aae1-cb3a6b22f8d1) | Important | Information Disclosure | 4011651 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2013 Service Pack 1 (64-bit editions) | [4011695 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c5ecb83f-e59f-4f82-acde-66f3cd7de3c3) | Important | Information Disclosure | 4011651 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2013 RT Service Pack 1 | 4011695 Security Update | Important | Information Disclosure | 4011651 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office Web Apps Server 2013 Service Pack 1 | [4011692 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=cb5a24eb-fb9b-4c73-9d94-d33a2a71b959) | Important | Information Disclosure | 4011648 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 for Mac | [Release Notes Security Update](https://go.microsoft.com/fwlink/p/?linkid=831049) | Important | Information Disclosure | 4011648 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Word 2016 (32-bit edition) | [4011730 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=7f489ea3-5766-4162-ba61-13f889a80f64) | Important | Information Disclosure | 4011643 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2016 (64-bit edition) | [4011730 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=0a8ac965-3b3c-48b0-a555-b60cf58c115d) | Important | Information Disclosure | 4011643 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office Online Server 2016 | [4011023 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=5968d892-8315-4623-aa8a-9a1cc660b643) | Important | Information Disclosure | 4011022 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions | Click to Run Security Update | Important | Information Disclosure | 4011022 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions | Click to Run Security Update | Important | Information Disclosure | 4011022 | Base: N/A Temporal: N/A Vector: N/A | No |
| Microsoft SharePoint Enterprise Server 2016 | [4018293 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75313053-6472-451e-8623-d125975f6fe7) | Important | Information Disclosure | 4011680 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2013 Service Pack 1 | [4011688 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=3e043e39-0cd3-4178-bc27-ec6e04a9be6f) | Important | Information Disclosure | 4011579 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0921 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0921 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0921) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0921) | **CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0921** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft SharePoint Enterprise Server 2016 | [4018293 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75313053-6472-451e-8623-d125975f6fe7) | Important | Elevation of Privilege | 4011680 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0922 - Microsoft Office Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0922 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0922) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0922) | **CVE Title:** Microsoft Office Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in Microsoft Office software when the Office software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.  Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file.  Note that the Preview Pane is not an attack vector for this vulnerability. The security update addresses the vulnerability by correcting how Office handles objects in memory.  **FAQ:**  **I have Microsoft Word 2010 installed. Why am I not being offered the 4011673 update?** The 4011673 update only applies to systems running specific configurations of Microsoft Office 2010. Some configurations will not be offered the update.  **I am being offered this update for software that is not specifically indicated as being affected in the Affected Software and Vulnerability Severity Ratings table. Why am I being offered this update?** When updates address vulnerable code that exists in a component that is shared between multiple Microsoft Office products or shared between multiple versions of the same Microsoft Office product, the update is considered to be applicable to all supported products and versions that contain the vulnerable component.  For example, when an update applies to Microsoft Office 2007 products, only Microsoft Office 2007 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2007, Microsoft Excel 2007, Microsoft Visio 2007, Microsoft Compatibility Pack, Microsoft Excel Viewer, or any other Microsoft Office 2007 product that is not specifically listed in the Affected Software table. Furthermore, when an update applies to Microsoft Office 2010 products, only Microsoft Office 2010 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2010, Microsoft Excel 2010, Microsoft Visio 2010, Microsoft Visio Viewer, or any other Microsoft Office 2010 product that is not specifically listed in the Affected Software table.  For more information on this behavior and recommended actions, see [Microsoft Knowledge Base Article 830335](https://support.microsoft.com/kb/830335). For a list of Microsoft Office products that an update may apply to, refer to the Microsoft Knowledge Base Article associated with the specific update.  **Why is there a separate update for Word Viewer** The Word Viewer update (4018309) is only supported, and will only install from Microsoft Update, if itâ€™s on Windows Embedded POSReady 2009. This is because Word Viewer ships pre-installed in Windows Embedded POSReady 2009, which is still in support. For other platforms, Word Viewer is no longer supported.  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0922** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Word 2007 Service Pack 3 | [4011721 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=f388529f-9558-4483-ba6f-7ac7d416f831) | Important | Remote Code Execution | 4011657 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2013 (32-bit editions) | [4011695 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=52c1a89e-7d46-462d-aae1-cb3a6b22f8d1) | Important | Remote Code Execution | 4011651 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2013 (64-bit editions) | [4011695 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c5ecb83f-e59f-4f82-acde-66f3cd7de3c3) | Important | Remote Code Execution | 4011651 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Server 2010 Service Pack 2 | [4011705 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=d124096c-8545-42d8-87a3-c7929abfa6bb) | Important | Remote Code Execution | 4011609 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2010 Service Pack 2 (32-bit editions) | [4011674 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=13ec5733-4eae-4e71-abe7-46c2bd292aa3) | Important | Remote Code Execution | 4011659 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2010 Service Pack 2 (64-bit editions) | [4011674 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=0689f54e-5e2b-42df-9ee5-56b0c150461c) | Important | Remote Code Execution | 4011659 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | [4011673 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=08f103c4-fa77-4156-af35-f89dca79bfbe) | Important | Remote Code Execution | 4011658 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | [4011673 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=ad50d12b-f9b6-4870-bc94-5d83879c2081) | Important | Remote Code Execution | 4011658 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office Web Apps 2010 Service Pack 2 | [4011709 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=f0bc5316-2a16-46fd-b2b8-23b237f8e662) | Important | Remote Code Execution | 4011615 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Word 2013 RT Service Pack 1 | 4011695 Security Update | Important | Remote Code Execution | 4011651 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office Web Apps 2013 Service Pack 1 | [4011692 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=cb5a24eb-fb9b-4c73-9d94-d33a2a71b959) | Important | Remote Code Execution | 4011648 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office Online Server 2016 | [4011023 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=5968d892-8315-4623-aa8a-9a1cc660b643) | Important | Remote Code Execution | 4011022 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2013 Service Pack 1 | [4011688 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=3e043e39-0cd3-4178-bc27-ec6e04a9be6f) | Important | Remote Code Execution | 4011579 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office Word Viewer | [4018309 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=3fcd76ab-73a3-49b3-b945-ab2ede6d3e5c) | Important | Remote Code Execution | 4011641 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Office Compatibility Pack Service Pack 3 | [4011720 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=3938bc12-645f-4b4d-b0e7-85914eaa0a67) | Important | Remote Code Execution | 4011607 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0923 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0923 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0923) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0923) | **CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0923** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft SharePoint Enterprise Server 2016 | [4018293 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75313053-6472-451e-8623-d125975f6fe7) | Important | Elevation of Privilege | 4011680 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2013 Service Pack 1 | [4018298 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=d3308910-45a1-488c-85b6-4e956515739b) | Important | Elevation of Privilege | 4011170 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0924 - Microsoft Exchange Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0924 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0924) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0924) | **CVE Title:** Microsoft Exchange Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the way that Microsoft Exchange Server handles URL redirects. If an impacted user is using Microsoft Exchange Outlook Web Access (OWA) Light, the vulnerability could allow an attacker to discover sensitive information that should otherwise not be disclosed, such as the URL of the user's OWA service.  To exploit the vulnerability, an attacker could embed a link in an email and send it to a victim. The attacker would then have to trick the user into clicking the link. The attacker would be unable to force the user to click the link.  The security update addresses the vulnerability by correcting how Microsoft Exchange handles URL redirects.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Low | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0924** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Exchange Server 2013 Service Pack 1 | [4073392 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=26753ad8-0261-45e7-b681-a732da52a806) | Low | Information Disclosure | 4036108 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2016 Cumulative Update 7 | [4073392 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=6369bd19-fcb2-4cb4-a4ee-a7d6c188cd6b) | Low | Information Disclosure | 4045655 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2013 Cumulative Update 18 | [4073392 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75ff9843-c036-4d39-bc7a-ea8bbed24879) | Low | Information Disclosure | 4045655 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2016 Cumulative Update 8 | [4073392 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=3b4dad74-9c89-47ec-be29-07934d1037c0) | Low | Information Disclosure | 4045655 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2013 Cumulative Update 19 | [4073392 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=f2b89ecd-f7fb-4785-8df3-3a3a1d95c34e) | Low | Information Disclosure | 4045655 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 20 | [4073537 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=378403b9-93be-4c01-b850-adf8a04684ec) | Low | Information Disclosure | 4035162 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0925 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0925 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0925) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0925) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.  If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  The security update addresses the vulnerability by modifying how the ChakraCore scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0925** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| ChakraCore | [Commit Security Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.2) | Critical | Remote Code Execution |  | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O | Yes |

# CVE-2018-0926 - Windows Kernel Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0926 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0926) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0926) | **CVE Title:** Windows Kernel Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.  To exploit this vulnerability, an authenticated attacker could run a specially crafted application. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.  The update addresses the vulnerability by correcting how the Windows kernel initializes objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0926** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0927 - Microsoft Browser Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0927 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0927) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0927) | **CVE Title:** Microsoft Browser Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when affected Microsoft browsers improperly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.  To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site.  The security update addresses the vulnerability by modifying how Microsoft browsers handle objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0927** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Important | Information Disclosure | 4074736 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Important | Information Disclosure | 4074736 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Information Disclosure | 4074736 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Important | Information Disclosure | 4074594 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Important | Information Disclosure | 4074594 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Low | Information Disclosure | 4074594 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Low | Information Disclosure | 4074590 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 10 on Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Information Disclosure | 4074736 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Low | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0929 - Internet Explorer Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0929 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0929) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0929) | **CVE Title:** Internet Explorer Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.  To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site.  The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0929** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Information Disclosure | 4074736 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Information Disclosure | 4074736 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Important | Information Disclosure | 4074736 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Important | Information Disclosure | 4074736 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Information Disclosure | 4074736 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Important | Information Disclosure | 4074594 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Important | Information Disclosure | 4074594 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Low | Information Disclosure | 4074594 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows RT 8.1 | 4088876 Monthly Rollup | Important | Information Disclosure | 4074594 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Information Disclosure | 4074596 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Information Disclosure | 4074591 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Low | Information Disclosure | 4074590 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Information Disclosure | 4074592 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 10 on Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Information Disclosure | 4074736 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0930 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0930 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0930) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0930) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0930** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Commit Security Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.2) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0931 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0931 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0931) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0931) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Moderate | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0931** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Remote Code Execution | 4074596 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Remote Code Execution | 4074596 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Moderate | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Commit Security Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.2) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0932 - Microsoft Browser Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0932 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0932) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0932) | **CVE Title:** Microsoft Browser Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when affected Microsoft browsers improperly handle objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system.  To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site.  The security update addresses the vulnerability by modifying how Microsoft browsers handle objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Critical | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0932** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Critical | Information Disclosure | 4074736 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Critical | Information Disclosure | 4074736 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Moderate | Information Disclosure | 4074736 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Critical | Information Disclosure | 4074594 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Critical | Information Disclosure | 4074594 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Moderate | Information Disclosure | 4074594 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows RT 8.1 | 4088876 Monthly Rollup | Critical | Information Disclosure | 4074594 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Information Disclosure | 4074596 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Information Disclosure | 4074596 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Information Disclosure | 4074591 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Information Disclosure | 4074591 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Moderate | Information Disclosure | 4074590 | Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Information Disclosure | 4074592 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Information Disclosure | 4074592 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Information Disclosure | 4074596 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Information Disclosure | 4074596 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Information Disclosure | 4074591 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Information Disclosure | 4074591 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Moderate | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Information Disclosure | 4074590 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Information Disclosure | 4074592 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Information Disclosure | 4074592 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0933 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0933 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0933) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0933) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0933** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Remote Code Execution | 4074596 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Remote Code Execution | 4074596 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Moderate | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Commit Security Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.2) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0934 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0934 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0934) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0934) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0934** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Remote Code Execution | 4074596 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Critical | Remote Code Execution | 4074596 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Critical | Remote Code Execution | 4074591 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Moderate | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Critical | Remote Code Execution | 4074590 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Commit Security Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.2) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0935 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0935 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0935) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0935) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0935** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Remote Code Execution | 4074736 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Remote Code Execution | 4074736 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Important | Remote Code Execution | 4074736 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Important | Remote Code Execution | 4074736 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Remote Code Execution | 4074736 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Important | Remote Code Execution | 4074594 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Important | Remote Code Execution | 4074594 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Low | Remote Code Execution | 4074594 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows RT 8.1 | 4088876 Monthly Rollup | Important | Remote Code Execution | 4074594 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Remote Code Execution | 4074596 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Remote Code Execution | 4074596 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Remote Code Execution | 4074591 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Remote Code Execution | 4074591 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Low | Remote Code Execution | 4074590 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Remote Code Execution | 4074590 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Remote Code Execution | 4074590 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Remote Code Execution | 4074592 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Remote Code Execution | 4074592 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Remote Code Execution | 4074588 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Remote Code Execution | 4074588 | Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Internet Explorer 10 on Windows Server 2012 | [4088877 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088877) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Remote Code Execution | 4074736 | Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0936 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0936 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0936) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0936) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0936** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Commit Security Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.2) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0937 - Chakra Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0937 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0937) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0937) | **CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability  **Description:**  A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.  The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Critical | Remote Code Execution |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0937** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Remote Code Execution | 4074592 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Commit Security Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.2) | Critical | Remote Code Execution | 4074588 | Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0939 - Scripting Engine Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0939 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0939) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0939) | **CVE Title:** Scripting Engine Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.  In a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site.  The security update addresses the vulnerability by changing how the scripting engine handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Critical | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0939** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Information Disclosure | 4074592 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Critical | Information Disclosure | 4074592 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Microsoft Edge on Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Critical | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| ChakraCore | [Commit Security Only](https://github.com/Microsoft/ChakraCore/releases/tag/v1.8.2) | Critical | Information Disclosure | 4074588 | Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0940 - Microsoft Exchange Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0940 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0940) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0940) | **CVE Title:** Microsoft Exchange Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft Exchange Outlook Web Access (OWA) fails to properly sanitize links presented to users. An attacker who successfully exploited this vulnerability could override the OWA interface with a fake login page and attempt to trick the user into disclosing sensitive information.  To exploit the vulnerability, an attacker could send a specially crafted email message containing a malicious link to a user. The user would have to click the malicious link in order to be susceptible to the vulnerability.  The security update addresses the vulnerability by correcting how Microsoft Exchange rewrites links presented within the body of emails.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Moderate | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0940** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Exchange Server 2013 Service Pack 1 | [4073392 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=26753ad8-0261-45e7-b681-a732da52a806) | Moderate | Elevation of Privilege | 4036108 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2016 Cumulative Update 7 | [4073392 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=6369bd19-fcb2-4cb4-a4ee-a7d6c188cd6b) | Moderate | Elevation of Privilege | 4045655 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2013 Cumulative Update 18 | [4073392 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75ff9843-c036-4d39-bc7a-ea8bbed24879) | Moderate | Elevation of Privilege | 4045655 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2016 Cumulative Update 8 | [4073392 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=3b4dad74-9c89-47ec-be29-07934d1037c0) | Moderate | Elevation of Privilege | 4045655 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2013 Cumulative Update 19 | [4073392 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=f2b89ecd-f7fb-4785-8df3-3a3a1d95c34e) | Moderate | Elevation of Privilege | 4045655 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 20 | [4073537 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=378403b9-93be-4c01-b850-adf8a04684ec) | Important | Elevation of Privilege | 4035162 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0941 - Microsoft Exchange Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0941 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0941) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0941) | **CVE Title:** Microsoft Exchange Information Disclosure Vulnerability  **Description:**  An information disclosure vulnerability exists in the way that Microsoft Exchange Server handles importing data. If an impacted user is using Microsoft Exchange Outlook Web Access (OWA), the vulnerability could allow an attacker to discover sensitive information that should otherwise not be disclosed.  To exploit the vulnerability, an attacker would have to upload a specially crafted file to Microsoft Exchange Outlook Web Access (OWA).  The security update addresses the vulnerability by correcting how Microsoft Exchange handles importing data.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Information Disclosure |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0941** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Exchange Server 2016 Cumulative Update 7 | [4073392 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=6369bd19-fcb2-4cb4-a4ee-a7d6c188cd6b) | Important | Information Disclosure | 4045655 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft Exchange Server 2016 Cumulative Update 8 | [4073392 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=3b4dad74-9c89-47ec-be29-07934d1037c0) | Important | Information Disclosure | 4045655 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0942 - Internet Explorer Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0942 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0942) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0942) | **CVE Title:** Internet Explorer Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Internet Explorer fails a check, allowing sandbox escape. An attacker who successfully exploited the vulnerability could use the sandbox escape to elevate privileges on an affected system.  This vulnerability by itself does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability (such as a remote code execution vulnerability or another elevation of privilege vulnerability) that is capable of leveraging the elevated privileges when code execution is attempted.  The update addresses the vulnerability by correcting how Internet Explorer handles zone and integrity settings.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Low | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0942** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Important | Elevation of Privilege | 4074736 | Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Important | Elevation of Privilege | 4074736 | Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4088875 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088875) [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) | Low | Elevation of Privilege | 4074736 | Base: 2.6 Temporal: 2.4 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for 32-bit systems | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Important | Elevation of Privilege | 4074594 | Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 8.1 for x64-based systems | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Important | Elevation of Privilege | 4074594 | Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2012 R2 | [4089187 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4089187) [4088876 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088876) | Low | Elevation of Privilege | 4074594 | Base: 2.6 Temporal: 2.4 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows RT 8.1 | 4088876 Monthly Rollup | Important | Elevation of Privilege | 4074594 | Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Elevation of Privilege | 4074596 | Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Elevation of Privilege | 4074596 | Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Elevation of Privilege | 4074591 | Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Elevation of Privilege | 4074591 | Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Low | Elevation of Privilege | 4074590 | Base: 2.6 Temporal: 2.4 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |
| Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C | Yes |

# CVE-2018-0944 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0944 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0944) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0944) | **CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0944** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Project Server 2013 Service Pack 1 | [4018305 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=427b7f98-069b-4ee8-869d-2b9ed74a1ae0) | Important | Elevation of Privilege | 4011701 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4018293 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75313053-6472-451e-8623-d125975f6fe7) | Important | Elevation of Privilege | 4011680 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0947 - Microsoft Sharepoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0947 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0947) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0947) | **CVE Title:** Microsoft Sharepoint Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly verify tenant permissions. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server.  The attacker who successfully exploited the vulnerability could elevate permssions such that they gain full rights to the affected tenant. These attacks could allow the attacker to read content that the attacker is not authorized to read, change permissions, and edit or delete content.  The security update addresses the vulnerability by helping to ensure that SharePoint Server properly checks tenant permissions.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0947** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft SharePoint Foundation 2013 Service Pack 1 | [4018304 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=0e70147e-281b-4db6-ac95-5833586972db) | Important | Elevation of Privilege | 4011653 | Base: N/A Temporal: N/A Vector: N/A | Maybe |
| Microsoft SharePoint Enterprise Server 2016 | [4018293 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=75313053-6472-451e-8623-d125975f6fe7) | Important | Elevation of Privilege | 4011680 | Base: N/A Temporal: N/A Vector: N/A | Maybe |

# CVE-2018-0977 - Win32k Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0977 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0977) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0977) | **CVE Title:** Win32k Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.  The update addresses this vulnerability by correcting how the Windows kernel-mode driver handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0977** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Elevation of Privilege | 4074596 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4088786 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088786) | Important | Elevation of Privilege | 4074596 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Elevation of Privilege | 4074591 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Elevation of Privilege | 4074591 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2018-0983 - Windows Storage Services Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2018-0983 [MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0983) [NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0983) | **CVE Title:** Windows Storage Services Elevation of Privilege Vulnerability  **Description:**  An elevation of privilege vulnerability exists when Storage Services improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context.  To exploit the vulnerability, an attacker would first have to log on to the system, and then run a specially crafted application to take control over the affected system.  The security update addresses the vulnerability by correcting how Storage Services handles objects in memory.  **FAQ:** None  **Mitigations:** None  **Workarounds:** None  **Revision:** 1.0    03/13/2018 07:00:00  Information published. | Important | Elevation of Privilege |

## Affected Software

The following tables list the affected software details for the vulnerability.

| **CVE-2018-0983** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 Version 1511 for x64-based Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Elevation of Privilege | 4074591 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1511 for 32-bit Systems | [4088779 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088779) | Important | Elevation of Privilege | 4074591 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for 32-bit Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1607 for x64-based Systems | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4088787 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088787) | Important | Elevation of Privilege | 4074590 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for 32-bit Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1703 for x64-based Systems | [4088782 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088782) | Important | Elevation of Privilege | 4074592 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for 32-bit Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 Version 1709 for x64-based Systems | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4088776 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4088776) | Important | Elevation of Privilege | 4074588 | Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

**声 明**

=============

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。

**关于绿盟科技**

==============

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于2000年4月，总部位于北京。在国内外设有30多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及Web安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于2014年1月29日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

 

绿盟科技官方微博二维码 绿盟科技官方微信二维码