**微软发布12月补丁修复37个安全问题**

**安全威胁通告**



发布时间：2017年12月13日

## 综述

微软于周二发布了12月安全更新补丁，修复了37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Adobe Flash Player、Device Guard、Microsoft Edge、Microsoft Exchange Server、Microsoft Malware Protection Engine、Microsoft Office、Microsoft Scripting Engine以及Microsoft Windows。

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 |
| Adobe Flash Player | ADV170022 | December 2017 Flash 安全更新 |
| Device Guard | CVE-2017-11899 | Microsoft Windows 安全功能绕过漏洞 |
| Microsoft Edge | CVE-2017-11888 | Microsoft Edge 内存破坏漏洞 |
| Microsoft Exchange Server | CVE-2017-11932 | Microsoft Exchange 欺骗漏洞 |
| Microsoft Exchange Server | ADV170023 | Microsoft Exchange Defense in Depth Update |
| Microsoft Malware Protection Engine | CVE-2017-11937 | Microsoft Malware Protection Engine 远程代码执行漏洞 |
| Microsoft Malware Protection Engine | CVE-2017-11940 | Microsoft Malware Protection Engine 远程代码执行漏洞 |
| Microsoft Office | ADV170021 | Microsoft Office Defense in Depth Update |
| Microsoft Office | CVE-2017-11934 | Microsoft PowerPoint 信息泄露漏洞 |
| Microsoft Office | CVE-2017-11935 | Microsoft Excel 远程代码执行漏洞 |
| Microsoft Office | CVE-2017-11936 | Microsoft SharePoint 特权提升漏洞 |
| Microsoft Office | CVE-2017-11939 | Microsoft Office 信息泄露漏洞 |
| Microsoft Scripting Engine | CVE-2017-11889 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11890 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11893 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11895 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11901 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11903 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11906 | Scripting Engine 信息泄露漏洞 |
| Microsoft Scripting Engine | CVE-2017-11908 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11909 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11910 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11911 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11912 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11913 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11914 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11918 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11930 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11886 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11887 | Scripting Engine 信息泄露漏洞 |
| Microsoft Scripting Engine | CVE-2017-11894 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11907 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11905 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11916 | Scripting Engine 内存破坏漏洞 |
| Microsoft Scripting Engine | CVE-2017-11919 | Scripting Engine 信息泄露漏洞 |
| Microsoft Windows | CVE-2017-11885 | Windows RRAS Service 远程代码执行漏洞 |
| Microsoft Windows | CVE-2017-11927 | Microsoft Windows 信息泄露漏洞 |

## 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

# ADV170021 - Microsoft Office Defense in Depth Update

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| ADV170021[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=ADV170021)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=ADV170021) | **CVE Title:** Microsoft Office Defense in Depth Update **Description:** Microsoft has released an update for Microsoft Office that provides enhanced security as a defense-in-depth measure. The update disables the Dynamic Update Exchange protocol (DDE) in all supported editions of Microsoft Word.Microsoft is continuing to investigate this issue and will update this advisory as further updates become available. If you are unable to install the update, or if you need to disable the DDE protocol in other Office applications such as Excel, see [Microsoft Security Advisory 4053440](https://docs.microsoft.com/en-us/security-updates/securityadvisories/2017/4053440). Note that the mitigations listed in the advisory will not disable DDE, but will disable auto-update for any linked fields, including DDE.If you need to change DDE functionality in Word after installing the update, follow these steps:1. In the Registry Editor navigate to \HKEY\_CURRENT\_USER\Software\Microsoft\Office\version\Word\Security AllowDDE(DWORD)
2. Set the DWORD value based on your requirements as follows:
* AllowDDE(DWORD) = 0: To disable DDE. This is the default setting after you install the update.
* AllowDDE(DWORD) = 1: To allow DDE requests to an already running program, but prevent DDE requests that require another executable program to be launched.
* AllowDDE(DWORD) = 2: To fully allow DDE requests.

**FAQ:****I have Microsoft Word 2010 installed. Why am I not being offered the 4011612 update?** The 4011612 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:****Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | None | Defense in Depth |

## Affected Software

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

| **ADV170021** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Word 2007 Service Pack 3 | [4011608 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=0f7fc545-099c-474b-b45b-0b92552d9817) | None | Defense in Depth | 4011266 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Word 2010 Service Pack 2 (32-bit editions) | [4011614 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=5a565fd4-473a-49ee-9500-03abe229b693) | None | Defense in Depth | 4011270 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Word 2010 Service Pack 2 (64-bit editions) | [4011614 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=0ae7bfd9-05d0-4050-86f7-079203d7509b) | None | Defense in Depth | 4011270 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (32-bit editions) | [4011612 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=60cbaeac-b79a-400e-b313-b6b82067177b) | None | Defense in Depth | 4011268 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Office 2010 Service Pack 2 (64-bit editions) | [4011612 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=5bb1788a-9c58-41bc-9d5a-e0a58d04bbdc) | None | Defense in Depth | 4011268 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Word 2013 Service Pack 1 (32-bit editions) | [4011590 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=4425c867-b27c-4efe-95e3-c3a319fb8ec6) | None | Defense in Depth | 4011250 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Word 2013 Service Pack 1 (64-bit editions) | [4011590 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=11adedec-fd39-4549-b0e2-b77ebfdf8087) | None | Defense in Depth | 4011250 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Word 2013 RT Service Pack 1 | 4011590 Security Update | None | Defense in Depth | 4011250 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Word 2016 (32-bit edition) | [4011575 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=45e2924e-0398-4aca-8971-95defd6fd731) | None | Defense in Depth | 4011242 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Word 2016 (64-bit edition) | [4011575 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=5f675e95-a075-4cad-8f1f-90b0268fca7a) | None | Defense in Depth | 4011242 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions | Click to Run Security Update | None | Defense in Depth | 4011242 | Base: N/ATemporal: N/AVector: N/A | No |
| Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions | Click to Run Security Update | None | Defense in Depth | 4011242 | Base: N/ATemporal: N/AVector: N/A | No |

# ADV170022 - December 2017 Flash Security Update

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| ADV170022[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=ADV170022)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=ADV170022) | **CVE Title:** December 2017 Flash Security Update **Description:** This security update addresses the following vulnerability, which is described in Adobe Security Bulletin [APSB17-42](http://helpx.adobe.com/security/products/flash-player/apsb17-42.html): CVE-2017-11305**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:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **ADV170022** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Adobe Flash Player on Windows Server 2012 | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows 8.1 for 32-bit systems | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows 8.1 for x64-based systems | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows Server 2012 R2 | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows RT 8.1 | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows 10 for 32-bit Systems | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows 10 for x64-based Systems | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1511 for x64-based Systems | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1511 for 32-bit Systems | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows Server 2016 | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1709 for 32-bit Systems | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows 10 Version 1709 for x64-based Systems | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Adobe Flash Player on Windows Server, version 1709 (Server Core Installation) | [4053577 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053577) | Critical | Remote Code Execution | 4049179 | Base: N/ATemporal: N/AVector: N/A | Yes |

# ADV170023 - Microsoft Exchange Defense in Depth Update

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| ADV170023[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=ADV170023)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=ADV170023) | **CVE Title:** Microsoft Exchange Defense in Depth Update **Description:** Microsoft has released an update for Microsoft Exchange that provides enhanced security as a defense-in-depth measure.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | None | Defense in Depth |

## Affected Software

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

| **ADV170023** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Exchange Server 2013 Cumulative Update 17 | [4045655 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=0fc11c77-5442-4a64-92c4-bce25675ad32) | None | Defense in Depth | 4036108 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Microsoft Exchange Server 2016 Cumulative Update 6 | [4045655 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=572eec81-2998-48a3-be54-f4a2d067f268) | None | Defense in Depth | 4036108 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Microsoft Exchange Server 2016 Cumulative Update 7 | [4045655 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c7db6072-e1be-4439-bbb3-b0cc13072fb7) | None | Defense in Depth | 4036108 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Microsoft Exchange Server 2013 Cumulative Update 18 | [4045655 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=9387fe84-723c-499b-b8b9-22e99aa910c0) | None | Defense in Depth | 4036108 | Base: N/ATemporal: N/AVector: N/A | Yes |

# CVE-2017-11885 - Windows RRAS Service Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11885[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11885)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11885) | **CVE Title:** Windows RRAS Service Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in RPC if the server has Routing and Remote Access enabled. An attacker who successfully exploited this vulnerability could execute code on the target system. 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 need to run a specially crafted application against an RPC server which has Routing and Remote Access enabled. Routing and Remote Access is a non-default configuration; systems without it enabled are not vulnerable.The security update addresses the vulnerability by correcting how the Routing and Remote Access service handles requests.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11885** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4054521 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054521) | Important | Remote Code Execution | 4048957 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4054521 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054521) | Important | Remote Code Execution | 4048957 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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) | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4054521 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054521) | Important | Remote Code Execution | 4048957 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4054521 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054521) | Important | Remote Code Execution | 4048957 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4054521 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054521) | Important | Remote Code Execution | 4048957 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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) | [4052303 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052303) | Important | Remote Code Execution | 4048957 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 | [4054520 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054520)[4054523 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054523) | Important | Remote Code Execution | 4048959 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 (Server Core installation) | [4054520 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054520)[4054523 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054523) | Important | Remote Code Execution | 4048959 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for 32-bit systems | [4054522 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054522)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Important | Remote Code Execution | 4048958 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 8.1 for x64-based systems | [4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519)[4054522 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054522) | Important | Remote Code Execution | 4048958 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 | [4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519)[4054522 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054522) | Important | Remote Code Execution | 4048958 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows RT 8.1 | 4054519 Monthly Rollup | Important | Remote Code Execution | 4048958 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2012 R2 (Server Core installation) | [4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519)[4054522 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054522) | Important | Remote Code Execution | 4048958 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for 32-bit Systems | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Remote Code Execution | 4048956 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows 10 for x64-based Systems | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Remote Code Execution | 4048956 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Remote Code Execution | 4048952 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Remote Code Execution | 4048952 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Remote Code Execution | 4048953 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Remote Code Execution | 4048953 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Remote Code Execution | 4048953 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server 2016 (Server Core installation) | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Remote Code Execution | 4048953 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Remote Code Execution | 4048954 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Remote Code Execution | 4048954 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Remote Code Execution | 4048955 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Remote Code Execution | 4048955 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |
| Windows Server, version 1709 (Server Core Installation) | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Remote Code Execution | 4048955 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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 | [4052303 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052303) | Important | Remote Code Execution | 4048955 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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 | [4052303 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052303) | Important | Remote Code Execution | 4048955 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/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) | [4052303 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052303) | Important | Remote Code Execution | 4048955 | Base: 6.6Temporal: 5.9Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C | Yes |

# CVE-2017-11886 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11886[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11886)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11886) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Internet Explorer improperly accesses 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, the attacker 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.An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding 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, typically by an enticement in an email or instant message, or by getting the user to open an attachment sent through email.The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Moderate | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11886** |
| --- |
| **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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Moderate | Remote Code Execution | 4047206 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Moderate | Remote Code Execution | 4047206 | Base: 6.4Temporal: 5.8Vector: 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 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Critical | Remote Code Execution | 4047206 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Critical | Remote Code Execution | 4048957 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Moderate | Remote Code Execution | 4048957 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Moderate | Remote Code Execution | 4048958 | Base: 6.4Temporal: 5.8Vector: 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 | 4054519 Monthly Rollup | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 6.4Temporal: 5.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054520 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054520) | Moderate | Remote Code Execution | 4048959 | Base: 6.4Temporal: 5.8Vector: 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-2017-11887 - Scripting Engine Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11887[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11887)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11887) | **CVE Title:** Scripting Engine 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    12/12/2017 08:00:00    Information published.  | Low | Information Disclosure |

## Affected Software

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

| **CVE-2017-11887** |
| --- |
| **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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Low | Information Disclosure | 4047206 | Base: 2.4Temporal: 2.2Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Low | Information Disclosure | 4047206 | Base: 2.4Temporal: 2.2Vector: 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 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Important | Information Disclosure | 4047206 | Base: 4.3Temporal: 3.9Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Important | Information Disclosure | 4048957 | Base: 4.3Temporal: 3.9Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Low | Information Disclosure | 4048957 | Base: 2.4Temporal: 2.2Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Important | Information Disclosure | 4048958 | Base: 4.3Temporal: 3.9Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Important | Information Disclosure | 4048958 | Base: 4.3Temporal: 3.9Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Low | Information Disclosure | 4048958 | Base: 2.4Temporal: 2.2Vector: 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 | 4054519 Monthly Rollup | Important | Information Disclosure | 4048958 | Base: 4.3Temporal: 3.9Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Information Disclosure | 4048956 | Base: 4.3Temporal: 3.9Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Information Disclosure | 4048956 | Base: 4.3Temporal: 3.9Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Information Disclosure | 4048952 | Base: 4.3Temporal: 3.9Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Information Disclosure | 4048952 | Base: 4.3Temporal: 3.9Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Low | Information Disclosure | 4048953 | Base: 2.4Temporal: 2.2Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Information Disclosure | 4048953 | Base: 4.3Temporal: 3.9Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Information Disclosure | 4048953 | Base: 4.3Temporal: 3.9Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Information Disclosure | 4048954 | Base: 4.3Temporal: 3.9Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Information Disclosure | 4048954 | Base: 4.3Temporal: 3.9Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Information Disclosure | 4048955 | Base: 4.3Temporal: 3.9Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Information Disclosure | 4048955 | Base: 4.3Temporal: 3.9Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054520 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054520) | Low | Information Disclosure | 4048959 | Base: 2.4Temporal: 2.2Vector: 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-2017-11888 - Microsoft Edge Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11888[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11888)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11888) | **CVE Title:** Microsoft Edge Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that enables an attacker to 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 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.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 by adding specially crafted content that could exploit the vulnerability. 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 way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email.The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11888** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11889 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11889[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11889)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11889) | **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    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11889** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11890 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11890[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11890)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11890) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Internet Explorer improperly accesses 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, the attacker 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.An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding 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, typically by an enticement in an email or instant message, or by getting the user to open an attachment sent through email.The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11890** |
| --- |
| **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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Moderate | Remote Code Execution | 4047206 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Moderate | Remote Code Execution | 4047206 | Base: 6.4Temporal: 5.8Vector: 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 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Critical | Remote Code Execution | 4047206 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Critical | Remote Code Execution | 4048957 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Moderate | Remote Code Execution | 4048957 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Moderate | Remote Code Execution | 4048958 | Base: 6.4Temporal: 5.8Vector: 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 | 4054519 Monthly Rollup | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 6.4Temporal: 5.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054520 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054520) | Moderate | Remote Code Execution | 4048959 | Base: 6.4Temporal: 5.8Vector: 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-2017-11893 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11893[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11893)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11893) | **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    12/12/2017 08:00:00    Information published.  | Moderate | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11893** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11894 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11894[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11894)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11894) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. 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 designed to exploit the vulnerability through a Microsoft browser 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 browser 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    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11894** |
| --- |
| **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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Moderate | Remote Code Execution | 4047206 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Moderate | Remote Code Execution | 4047206 | Base: 6.4Temporal: 5.8Vector: 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 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Critical | Remote Code Execution | 4047206 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Critical | Remote Code Execution | 4048957 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Moderate | Remote Code Execution | 4048957 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Moderate | Remote Code Execution | 4048958 | Base: 6.4Temporal: 5.8Vector: 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 | 4054519 Monthly Rollup | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 6.4Temporal: 5.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054520 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054520) | Moderate | Remote Code Execution | 4048959 | Base: 6.4Temporal: 5.8Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11895 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11895[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11895)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11895) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. 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 designed to exploit the vulnerability through a Microsoft browser 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 browser 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    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11895** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Critical | Remote Code Execution | 4047206 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Critical | Remote Code Execution | 4048957 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Moderate | Remote Code Execution | 4048957 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Moderate | Remote Code Execution | 4048958 | Base: 6.4Temporal: 5.8Vector: 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 | 4054519 Monthly Rollup | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 6.4Temporal: 5.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11899 - Microsoft Windows Security Feature Bypass Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11899[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11899)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11899) | **CVE Title:** Microsoft Windows Security Feature Bypass Vulnerability **Description:** A security feature bypass exists when Device Guard incorrectly validates an untrusted file. An attacker who successfully exploited this vulnerability could make an unsigned file appear to be signed. Because Device Guard relies on the signature to determine the file is non-malicious, Device Guard could then allow a malicious file to execute.In an attack scenario, an attacker could make an untrusted file appear to be a trusted file.The update addresses the vulnerability by correcting how Device Guard handles untrusted files.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Important | Security Feature Bypass |

## Affected Software

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

| **CVE-2017-11899** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 10 for 32-bit Systems | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Security Feature Bypass | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 |
| Windows 10 for x64-based Systems | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Security Feature Bypass | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 |
| Windows 10 Version 1511 for x64-based Systems | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Security Feature Bypass | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 |
| Windows 10 Version 1511 for 32-bit Systems | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Security Feature Bypass | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 |
| Windows Server 2016 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Security Feature Bypass | 4048953 | Base: 6.4Temporal: 5.8Vector: 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 |
| Windows 10 Version 1607 for 32-bit Systems | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Security Feature Bypass | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 |
| Windows 10 Version 1607 for x64-based Systems | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Security Feature Bypass | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 |
| Windows Server 2016 (Server Core installation) | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Security Feature Bypass | 4048953 | Base: 6.4Temporal: 5.8Vector: 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 |
| Windows 10 Version 1703 for 32-bit Systems | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Security Feature Bypass | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 |
| Windows 10 Version 1703 for x64-based Systems | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Security Feature Bypass | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 |
| Windows 10 Version 1709 for 32-bit Systems | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Security Feature Bypass | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 |
| Windows 10 Version 1709 for x64-based Systems | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Security Feature Bypass | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 |
| Windows Server, version 1709 (Server Core Installation) | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Security Feature Bypass | 4048955 | Base: 6.4Temporal: 5.8Vector: 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-2017-11901 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11901[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11901)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11901) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Internet Explorer improperly accesses 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, the attacker 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.An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding 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, typically by an enticement in an email or instant message, or by getting the user to open an attachment sent through email.The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11901** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Critical | Remote Code Execution | 4047206 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Critical | Remote Code Execution | 4048957 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Moderate | Remote Code Execution | 4048957 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Moderate | Remote Code Execution | 4048958 | Base: 6.4Temporal: 5.8Vector: 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 | 4054519 Monthly Rollup | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 6.4Temporal: 5.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054520 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054520) | Moderate | Remote Code Execution | 4048959 | Base: 6.4Temporal: 5.8Vector: 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-2017-11903 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11903[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11903)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11903) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Internet Explorer improperly accesses 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, the attacker 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.An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding 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, typically by an enticement in an email or instant message, or by getting the user to open an attachment sent through email.The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11903** |
| --- |
| **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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Moderate | Remote Code Execution | 4047206 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Moderate | Remote Code Execution | 4047206 | Base: 6.4Temporal: 5.8Vector: 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 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Critical | Remote Code Execution | 4047206 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Critical | Remote Code Execution | 4048957 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Moderate | Remote Code Execution | 4048957 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Moderate | Remote Code Execution | 4048958 | Base: 6.4Temporal: 5.8Vector: 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 | 4054519 Monthly Rollup | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 6.4Temporal: 5.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054520 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054520) | Moderate | Remote Code Execution | 4048959 | Base: 6.4Temporal: 5.8Vector: 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-2017-11905 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11905[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11905)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11905) | **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    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11905** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11906 - Scripting Engine Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11906[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11906)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11906) | **CVE Title:** Scripting Engine 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    12/12/2017 08:00:00    Information published.  | Low | Information Disclosure |

## Affected Software

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

| **CVE-2017-11906** |
| --- |
| **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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Low | Information Disclosure | 4047206 | Base: 2.4Temporal: 2.2Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Low | Information Disclosure | 4047206 | Base: 2.4Temporal: 2.2Vector: 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 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Important | Information Disclosure | 4047206 | Base: 4.3Temporal: 3.9Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Important | Information Disclosure | 4048957 | Base: 4.3Temporal: 3.9Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Low | Information Disclosure | 4048957 | Base: 2.4Temporal: 2.2Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Important | Information Disclosure | 4048958 | Base: 4.3Temporal: 3.9Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Important | Information Disclosure | 4048958 | Base: 4.3Temporal: 3.9Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Low | Information Disclosure | 4048958 | Base: 2.4Temporal: 2.2Vector: 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 | 4054519 Monthly Rollup | Important | Information Disclosure | 4048958 | Base: 4.3Temporal: 3.9Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Information Disclosure | 4048956 | Base: 4.3Temporal: 3.9Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Information Disclosure | 4048956 | Base: 4.3Temporal: 3.9Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Information Disclosure | 4048952 | Base: 4.3Temporal: 3.9Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Information Disclosure | 4048952 | Base: 4.3Temporal: 3.9Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Low | Information Disclosure | 4048953 | Base: 2.4Temporal: 2.2Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Information Disclosure | 4048953 | Base: 4.3Temporal: 3.9Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Information Disclosure | 4048953 | Base: 4.3Temporal: 3.9Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Information Disclosure | 4048954 | Base: 4.3Temporal: 3.9Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Information Disclosure | 4048954 | Base: 4.3Temporal: 3.9Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Information Disclosure | 4048955 | Base: 4.3Temporal: 3.9Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Information Disclosure | 4048955 | Base: 4.3Temporal: 3.9Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054520 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054520) | Low | Information Disclosure | 4048959 | Base: 2.4Temporal: 2.2Vector: 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-2017-11907 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11907[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11907)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11907) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Internet Explorer improperly accesses 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, the attacker 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.An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding 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, typically by an enticement in an email or instant message, or by getting the user to open an attachment sent through email.The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11907** |
| --- |
| **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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Moderate | Remote Code Execution | 4047206 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Moderate | Remote Code Execution | 4047206 | Base: 6.4Temporal: 5.8Vector: 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 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Critical | Remote Code Execution | 4047206 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Critical | Remote Code Execution | 4048957 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Moderate | Remote Code Execution | 4048957 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Moderate | Remote Code Execution | 4048958 | Base: 6.4Temporal: 5.8Vector: 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 | 4054519 Monthly Rollup | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 6.4Temporal: 5.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054520 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054520) | Moderate | Remote Code Execution | 4048959 | Base: 6.4Temporal: 5.8Vector: 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-2017-11908 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11908[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11908)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11908) | **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    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11908** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11909 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11909[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11909)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11909) | **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    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11909** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11910 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11910[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11910)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11910) | **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    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11910** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11911 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11911[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11911)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11911) | **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    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11911** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11912 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11912[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11912)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11912) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. 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 designed to exploit the vulnerability through a Microsoft browser 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 browser 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    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11912** |
| --- |
| **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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Moderate | Remote Code Execution | 4047206 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Moderate | Remote Code Execution | 4047206 | Base: 6.4Temporal: 5.8Vector: 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 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Critical | Remote Code Execution | 4047206 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Critical | Remote Code Execution | 4048957 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Moderate | Remote Code Execution | 4048957 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Moderate | Remote Code Execution | 4048958 | Base: 6.4Temporal: 5.8Vector: 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 | 4054519 Monthly Rollup | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 6.4Temporal: 5.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054520 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054520) | Moderate | Remote Code Execution | 4048959 | Base: 6.4Temporal: 5.8Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11913 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11913[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11913)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11913) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Internet Explorer improperly accesses 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, the attacker 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.An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding 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, typically by an enticement in an email or instant message, or by getting the user to open an attachment sent through email.The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11913** |
| --- |
| **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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Low | Remote Code Execution | 4047206 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Low | Remote Code Execution | 4047206 | Base: 6.4Temporal: 5.8Vector: 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 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Important | Remote Code Execution | 4047206 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Important | Remote Code Execution | 4048957 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Low | Remote Code Execution | 4048957 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Important | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Important | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Low | Remote Code Execution | 4048958 | Base: 6.4Temporal: 5.8Vector: 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 | 4054519 Monthly Rollup | Important | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Low | Remote Code Execution | 4048953 | Base: 6.4Temporal: 5.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054520 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054520) | Low | Remote Code Execution | 4048959 | Base: 6.4Temporal: 5.8Vector: 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-2017-11914 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11914[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11914)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11914) | **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    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11914** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 Version 1511 for x64-based Systems | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11916 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11916[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11916)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11916) | **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    12/12/2017 08:00:00    Information published.  | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11916** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| ChakraCore | [Commit Security Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Important | Remote Code Execution |  | Base: 4.2Temporal: 3.8Vector: 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-2017-11918 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11918[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11918)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11918) | **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    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11918** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Critical | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11919 - Scripting Engine Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11919[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11919)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11919) | **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    12/12/2017 08:00:00    Information published.  | Important | Information Disclosure |

## Affected Software

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

| **CVE-2017-11919** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Important | Information Disclosure | 4047206 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Important | Information Disclosure | 4048957 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Low | Information Disclosure | 4048957 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Important | Information Disclosure | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Important | Information Disclosure | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Low | Information Disclosure | 4048958 | Base: 6.4Temporal: 5.8Vector: 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 | 4054519 Monthly Rollup | Important | Information Disclosure | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Information Disclosure | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Information Disclosure | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Information Disclosure | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Information Disclosure | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Low | Information Disclosure | 4048953 | Base: 6.4Temporal: 5.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Information Disclosure | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Information Disclosure | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Information Disclosure | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Information Disclosure | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Information Disclosure | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Information Disclosure | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 |
| Microsoft Edge on Windows 10 for 32-bit Systems | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Information Disclosure | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Information Disclosure | 4048956 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Information Disclosure | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Information Disclosure | 4048952 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Low | Information Disclosure | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Information Disclosure | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Information Disclosure | 4048953 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Information Disclosure | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Information Disclosure | 4048954 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Information Disclosure | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Information Disclosure | 4048955 | Base: 4.2Temporal: 3.8Vector: 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 Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Important | Information Disclosure | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11927 - Microsoft Windows Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11927[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11927)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11927) | **CVE Title:** Microsoft Windows Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows its:// protocol handler unnecessarily sends traffic to a remote site in order to determine the zone of a provided URL. This could potentially result in the disclosure of sensitive information to a malicious site.To exploit the vulnerability an attacker would have to trick a user into browsing to a malicious website or to an SMB or UNC path destination. An attacker who successfully tricked a user into disclosing the user's NTLM hash could attempt a brute-force attack to disclose the corresponding hash password.The security update addresses the vulnerability by correcting how the Windows its:// protocol handler determines the zone of a request.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Important | Information Disclosure |

## Affected Software

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

| **CVE-2017-11927** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Windows 7 for 32-bit Systems Service Pack 1 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4054521 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054521) | Important | Information Disclosure | 4048957 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows 7 for x64-based Systems Service Pack 1 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4054521 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054521) | Important | Information Disclosure | 4048957 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4054521 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054521) | Important | Information Disclosure | 4048957 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4054521 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054521) | Important | Information Disclosure | 4048957 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4054521 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054521) | Important | Information Disclosure | 4048957 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) | [4053473 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053473) | Important | Information Disclosure | 4048957 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server 2012 | [4054520 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054520)[4054523 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054523) | Important | Information Disclosure | 4048959 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server 2012 (Server Core installation) | [4054520 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054520)[4054523 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054523) | Important | Information Disclosure | 4048959 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows 8.1 for 32-bit systems | [4054522 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054522)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Important | Information Disclosure | 4048958 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows 8.1 for x64-based systems | [4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519)[4054522 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054522) | Important | Information Disclosure | 4048958 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server 2012 R2 | [4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519)[4054522 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054522) | Important | Information Disclosure | 4048958 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows RT 8.1 | 4054519 Monthly Rollup | Important | Information Disclosure | 4048958 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server 2012 R2 (Server Core installation) | [4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519)[4054522 Security Only](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054522) | Important | Information Disclosure | 4048958 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows 10 for 32-bit Systems | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Information Disclosure | 4048956 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows 10 for x64-based Systems | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Important | Information Disclosure | 4048956 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows 10 Version 1511 for x64-based Systems | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Information Disclosure | 4048952 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows 10 Version 1511 for 32-bit Systems | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Important | Information Disclosure | 4048952 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server 2016 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Information Disclosure | 4048953 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows 10 Version 1607 for 32-bit Systems | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Information Disclosure | 4048955 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows 10 Version 1607 for x64-based Systems | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Information Disclosure | 4048953 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server 2016 (Server Core installation) | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Important | Information Disclosure | 4048953 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows 10 Version 1703 for 32-bit Systems | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Information Disclosure | 4048954 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows 10 Version 1703 for x64-based Systems | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Important | Information Disclosure | 4048954 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows 10 Version 1709 for 32-bit Systems | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Information Disclosure | 4048955 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows 10 Version 1709 for x64-based Systems | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Information Disclosure | 4048955 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server, version 1709 (Server Core Installation) | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Important | Information Disclosure | 4048955 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server 2008 for Itanium-Based Systems Service Pack 2 | [4053473 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053473) | Important | Information Disclosure | 4048955 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server 2008 for 32-bit Systems Service Pack 2 | [4053473 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053473) | Important | Information Disclosure | 4048955 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server 2008 for x64-based Systems Service Pack 2 | [4053473 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053473) | Important | Information Disclosure | 4048955 | Base: 4.3Temporal: 3.9Vector: 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 |
| Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) | [4053473 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053473) | Important | Information Disclosure | 4048955 | Base: 4.3Temporal: 3.9Vector: 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-2017-11930 - Scripting Engine Memory Corruption Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11930[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11930)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11930) | **CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers. 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 designed to exploit the vulnerability through a Microsoft browser 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 browser 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    12/12/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11930** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1 | [4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518)[4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978) | Critical | Remote Code Execution | 4047206 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Critical | Remote Code Execution | 4048957 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054518 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054518) | Moderate | Remote Code Execution | 4048957 | Base: 6.4Temporal: 5.8Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4052978 IE Cumulative](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4052978)[4054519 Monthly Rollup](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054519) | Moderate | Remote Code Execution | 4048958 | Base: 6.4Temporal: 5.8Vector: 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 | 4054519 Monthly Rollup | Critical | Remote Code Execution | 4048958 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053581 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053581) | Critical | Remote Code Execution | 4048956 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053578 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053578) | Critical | Remote Code Execution | 4048952 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Moderate | Remote Code Execution | 4048953 | Base: 6.4Temporal: 5.8Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053579 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053579) | Critical | Remote Code Execution | 4048953 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4053580 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4053580) | Critical | Remote Code Execution | 4048954 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 | [4054517 Security Update](https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4054517) | Critical | Remote Code Execution | 4048955 | Base: 7.5Temporal: 6.7Vector: 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 |
| ChakraCore | [Commit Security Update](https://github.com/Microsoft/ChakraCore/releases/tag/v1.7.5) | Important | Remote Code Execution | 4048955 | Base: 4.2Temporal: 3.8Vector: 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-2017-11932 - Microsoft Exchange Spoofing Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11932[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11932)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11932) | **CVE Title:** Microsoft Exchange Spoofing Vulnerability **Description:** A spoofing vulnerability exists in Microsoft Exchange Server when Outlook Web Access (OWA) fails to properly handle web requests. An attacker who successfully exploited the vulnerability could perform script or content injection attacks, and attempt to trick the user into disclosing sensitive information. An attacker could also redirect the user to a malicious website that could spoof content or be used as a pivot to chain an attack with other vulnerabilities in web services.To exploit the vulnerability, an attacker could send a specially crafted email containing a malicious link to a user. An attacker could also use a chat client to social engineer a user into clicking the malicious link. However, in both examples the user must click the malicious link. The security update addresses the vulnerability by correcting how OWA validates web requests.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Important | Spoofing |

## Affected Software

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

| **CVE-2017-11932** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Exchange Server 2016 Cumulative Update 6 | [4045655 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=572eec81-2998-48a3-be54-f4a2d067f268) | Important | Spoofing | 4036108 | Base: N/ATemporal: N/AVector: N/A | Yes |
| Microsoft Exchange Server 2016 Cumulative Update 7 | [4045655 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=c7db6072-e1be-4439-bbb3-b0cc13072fb7) | Important | Spoofing | 4036108 | Base: N/ATemporal: N/AVector: N/A | Yes |

# CVE-2017-11934 - Microsoft PowerPoint Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11934[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11934)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11934) | **CVE Title:** Microsoft PowerPoint Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory. An attacker who exploited the vulnerability could use the information to compromise the userâ€™s computer or data.To exploit the vulnerability, an attacker could craft a special document file and then convince the user to open it. An attacker must know the memory address location where the object was created.The update addresses the vulnerability by changing the way certain functions handle objects in memory.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Important | Information Disclosure |

## Affected Software

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

| **CVE-2017-11934** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2013 Service Pack 1 (32-bit editions) | [4011277 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=06e79630-6601-4e46-a8a6-db96fea5e704) | Important | Information Disclosure | 2975808 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Office 2013 Service Pack 1 (64-bit editions) | [4011277 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=91f18b74-6ff7-4155-b8f9-23faedaa877b) | Important | Information Disclosure | 2975808 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Office 2013 RT Service Pack 1 | 4011277 Security Update | Important | Information Disclosure | 2975808 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Office 2016 for Mac | [Release Notes Security Update](https://go.microsoft.com/fwlink/p/?linkid=831049) | Important | Information Disclosure | 2975808 | Base: N/ATemporal: N/AVector: N/A | No |
| Microsoft Office 2016 (32-bit edition) | [4011095 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=d0c17df1-ea42-46f0-9221-9e003574b40b) | Important | Information Disclosure | 2975808 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Office 2016 (64-bit edition) | [4011095 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=83a5c529-ddc2-4a3f-86b3-7400967002b3) | Important | Information Disclosure | 2975808 | Base: N/ATemporal: N/AVector: N/A | Maybe |
| Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions | Click to Run Security Update | Important | Information Disclosure | 2975808 | Base: N/ATemporal: N/AVector: N/A | No |
| Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions | Click to Run Security Update | Important | Information Disclosure | 2975808 | Base: N/ATemporal: N/AVector: N/A | No |

# CVE-2017-11935 - Microsoft Excel Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11935[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11935)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11935) | **CVE Title:** Microsoft Excel Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user.To exploit the vulnerability, a user must 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 that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the 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 correcting how Microsoft Office handles files in memory.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Important | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11935** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions | Click to Run Security Update | Important | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A | No |
| Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions | Click to Run Security Update | Important | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A | No |

# CVE-2017-11936 - Microsoft SharePoint Elevation of Privilege Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11936[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11936)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11936) | **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    12/12/2017 08:00:00    Information published.  | Important | Elevation of Privilege |

## Affected Software

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

| **CVE-2017-11936** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft SharePoint Enterprise Server 2016 | [4011576 Security Update](https://www.microsoft.com/downloads/details.aspx?familyid=dd16461c-5fec-4ec9-9c21-f48592d8ecfd) | Important | Elevation of Privilege | 4011244 | Base: N/ATemporal: N/AVector: N/A | Maybe |

# CVE-2017-11937 - Microsoft Malware Protection Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11937[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11937)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11937) | **CVE Title:** Microsoft Malware Protection Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Microsoft Malware Protection Engine does not properly scan a specially crafted file, leading to memory corruption. An attacker who successfully exploited this vulnerability could execute arbitrary code in the security context of the LocalSystem account and take control of the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.To exploit this vulnerability, a specially crafted file must be scanned by an affected version of the Microsoft Malware Protection Engine. There are many ways that an attacker could place a specially crafted file in a location that is scanned by the Microsoft Malware Protection Engine. For example, an attacker could use a website to deliver a specially crafted file to the victim's system that is scanned when the website is viewed by the user. An attacker could also deliver a specially crafted file via an email message or in an Instant Messenger message that is scanned when the file is opened. In addition, an attacker could take advantage of websites that accept or host user-provided content, to upload a specially crafted file to a shared location that is scanned by the Malware Protection Engine running on the hosting server.If the affected antimalware software has real-time protection turned on, the Microsoft Malware Protection Engine will scan files automatically, leading to exploitation of the vulnerability when the specially crafted file is scanned. If real-time scanning is not enabled, the attacker would need to wait until a scheduled scan occurs in order for the vulnerability to be exploited. All systems running an affected version of antimalware software are primarily at risk.The update addresses the vulnerability by correcting the manner in which the Microsoft Malware Protection Engine scans specially crafted files.Note: Typically, no action is required of enterprise administrators or end users to install updates for the Microsoft Malware Protection Engine, because the built-in mechanism for the automatic detection and deployment of updates will apply the update within 48 hours of release. The exact time frame depends on the software used, Internet connection, and infrastructure configuration.**FAQ:**

| **References** | **Identification** |
| --- | --- |
| Last version of the Microsoft Malware Protection Engine affected by this vulnerability | Version 1.1.14306.0 |
| First version of the Microsoft Malware Protection Engine with this vulnerability addressed | Version 1.1.14405.2 |

**Were active attacks detected using this vulnerability?** Microsoft is not aware of active attacks using this vulnerability.**Why was this released before the normal December Security Update Release on December 12, 2017** The Microsoft Malware Protection Engine is released along with anitmalware signatures. These releases donâ€™t always contain security updates and are not bound to a monthly cadence.**Why is no action required to install this update?** In response to a constantly changing threat landscape, Microsoft frequently updates malware definitions and the Microsoft Malware Protection Engine. In order to be effective in helping protect against new and prevalent threats, antimalware software must be kept up to date with these updates in a timely manner.For enterprise deployments as well as end users, the default configuration in Microsoft antimalware software helps ensure that malware definitions and the Microsoft Malware Protection Engine are kept up to date automatically. Product documentation also recommends that products are configured for automatic updating.Best practices recommend that customers regularly verify whether software distribution, such as the automatic deployment of Microsoft Malware Protection Engine updates and malware definitions, is working as expected in their environment.**How often are the Microsoft Malware Protection Engine and malware definitions updated?** Microsoft typically releases an update for the Microsoft Malware Protection Engine once a month or as needed to protect against new threats. Microsoft also typically updates the malware definitions three times daily and can increase the frequency when needed.Depending on which Microsoft antimalware software is used and how it is configured, the software may search for engine and definition updates every day when connected to the Internet, up to multiple times daily. Customers can also choose to manually check for updates at any time.**What is the Microsoft Malware Protection Engine?** The Microsoft Malware Protection Engine, mpengine.dll, provides the scanning, detection, and cleaning capabilities for Microsoft antivirus and antispyware software.**Does this update contain any additional security-related changes to functionality?** Yes. In addition to the changes that are listed for this vulnerability, this update includes defense-in-depth updates to help improve security-related features.**Where can I find more information about Microsoft antimalware technology?** For more information, visit the [Microsoft Malware Protection Center](https://www.microsoft.com/security/portal/) website.**Suggested Actions****Verify that the update is installed** Customers should verify that the latest version of the Microsoft Malware Protection Engine and definition updates are being actively downloaded and installed for their Microsoft antimalware products.For more information on how to verify the version number for the Microsoft Malware Protection Engine that your software is currently using, see the section, "Verifying Update Installation", in [Microsoft Knowledge Base Article 2510781](https://support.microsoft.com/kb/2510781).For affected software, verify that the Microsoft Malware Protection Engine version is 1.1.14405.2 or later.**If necessary, install the update** Administrators of enterprise antimalware deployments should ensure that their update management software is configured to automatically approve and distribute engine updates and new malware definitions. Enterprise administrators should also verify that the latest version of the Microsoft Malware Protection Engine and definition updates are being actively downloaded, approved and deployed in their environment.For end-users, the affected software provides built-in mechanisms for the automatic detection and deployment of this update. For these customers, the update will be applied within 48 hours of its availability. The exact time frame depends on the software used, Internet connection, and infrastructure configuration. End users that do not wish to wait can manually update their antimalware software.For more information on how to manually update the Microsoft Malware Protection Engine and malware definitions, refer to [Microsoft Knowledge Base Article 2510781](https://support.microsoft.com/kb/2510781).**Mitigations:****Workarounds:**None **Revision:**1.0    12/06/2017 08:00:00    Information published.1.2    12/12/2017 08:00:00    Changed Microsoft Forefront Endpoint Protection to Microsoft System Center Endpoint Protection in the Affected Products table.1.1    12/08/2017 08:00:00    Added information to the Frequently Asked Questions.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11937** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Security Essentials |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Intune Endpoint Protection |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Microsoft Exchange Server 2013 |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Microsoft Exchange Server 2016 |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Microsoft Forefront Endpoint Protection 2010 |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Microsoft System Center Endpoint Protection |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 7 for 32-bit Systems Service Pack 1 |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 7 for x64-based Systems Service Pack 1 |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 8.1 for 32-bit systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 8.1 for x64-based systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows RT 8.1 |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1511 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1511 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows Server 2016 |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1607 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1607 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows Server 2016 (Server Core installation) |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1703 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1703 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1709 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1709 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows Server, version 1709 (Server Core Installation) |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |

# CVE-2017-11939 - Microsoft Office Information Disclosure Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11939[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11939)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11939) | **CVE Title:** Microsoft Office Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Outlook fails to enforce copy/paste permissions on DRM-protected emails. An attacker who successfully exploited the vulnerability could potentially extract plaintext content from DRM-protected draft emails.The attacker would have to use another vulnerability to gain access to the victim's Drafts folder, either locally on the victim's system or remotely via MAPI.The security update addresses the vulnerability by correcting how Microsoft Outlook enforces DRM copy/paste permissions.**FAQ:**None **Mitigations:**None **Workarounds:**None **Revision:**1.0    12/12/2017 08:00:00    Information published.  | Important | Information Disclosure |

## Affected Software

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

| **CVE-2017-11939** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions | Click to Run Security Update | Important | Information Disclosure |  | Base: N/ATemporal: N/AVector: N/A | No |
| Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions | Click to Run Security Update | Important | Information Disclosure |  | Base: N/ATemporal: N/AVector: N/A | No |

# CVE-2017-11940 - Microsoft Malware Protection Engine Remote Code Execution Vulnerability

| **CVE ID** | **Vulnerability Description** | **Maximum Severity Rating** | **Vulnerability Impact** |
| --- | --- | --- | --- |
| CVE-2017-11940[MITRE](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11940)[NVD](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11940) | **CVE Title:** Microsoft Malware Protection Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Microsoft Malware Protection Engine does not properly scan a specially crafted file, leading to memory corruption. An attacker who successfully exploited this vulnerability could execute arbitrary code in the security context of the LocalSystem account and take control of the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.To exploit this vulnerability, a specially crafted file must be scanned by an affected version of the Microsoft Malware Protection Engine. There are many ways that an attacker could place a specially crafted file in a location that is scanned by the Microsoft Malware Protection Engine. For example, an attacker could use a website to deliver a specially crafted file to the victim's system that is scanned when the website is viewed by the user. An attacker could also deliver a specially crafted file via an email message or in an Instant Messenger message that is scanned when the file is opened. In addition, an attacker could take advantage of websites that accept or host user-provided content, to upload a specially crafted file to a shared location that is scanned by the Malware Protection Engine running on the hosting server.If the affected antimalware software has real-time protection turned on, the Microsoft Malware Protection Engine will scan files automatically, leading to exploitation of the vulnerability when the specially crafted file is scanned. If real-time scanning is not enabled, the attacker would need to wait until a scheduled scan occurs in order for the vulnerability to be exploited. All systems running an affected version of antimalware software are primarily at risk.The update addresses the vulnerability by correcting the manner in which the Microsoft Malware Protection Engine scans specially crafted files.Note: Typically, no action is required of enterprise administrators or end users to install updates for the Microsoft Malware Protection Engine, because the built-in mechanism for the automatic detection and deployment of updates will apply the update within 48 hours of release. The exact time frame depends on the software used, Internet connection, and infrastructure configuration.**FAQ:**

| **References** | **Identification** |
| --- | --- |
| Last version of the Microsoft Malware Protection Engine affected by this vulnerability | Version 1.1.14306.0 |
| First version of the Microsoft Malware Protection Engine with this vulnerability addressed | Version 1.1.14405.2 |

**Were active attacks detected using this vulnerability?** Microsoft is not aware of active attacks using this vulnerability.**Why was this released before the normal December Security Update Release on December 12, 2017** The Microsoft Malware Protection Engine is released along with anitmalware signatures. These releases donâ€™t always contain security updates and are not bound to a monthly cadence.**Why is no action required to install this update?** In response to a constantly changing threat landscape, Microsoft frequently updates malware definitions and the Microsoft Malware Protection Engine. In order to be effective in helping protect against new and prevalent threats, antimalware software must be kept up to date with these updates in a timely manner.For enterprise deployments as well as end users, the default configuration in Microsoft antimalware software helps ensure that malware definitions and the Microsoft Malware Protection Engine are kept up to date automatically. Product documentation also recommends that products are configured for automatic updating.Best practices recommend that customers regularly verify whether software distribution, such as the automatic deployment of Microsoft Malware Protection Engine updates and malware definitions, is working as expected in their environment.**How often are the Microsoft Malware Protection Engine and malware definitions updated?** Microsoft typically releases an update for the Microsoft Malware Protection Engine once a month or as needed to protect against new threats. Microsoft also typically updates the malware definitions three times daily and can increase the frequency when needed.Depending on which Microsoft antimalware software is used and how it is configured, the software may search for engine and definition updates every day when connected to the Internet, up to multiple times daily. Customers can also choose to manually check for updates at any time.**What is the Microsoft Malware Protection Engine?** The Microsoft Malware Protection Engine, mpengine.dll, provides the scanning, detection, and cleaning capabilities for Microsoft antivirus and antispyware software.**Does this update contain any additional security-related changes to functionality?** Yes. In addition to the changes that are listed for this vulnerability, this update includes defense-in-depth updates to help improve security-related features.**Where can I find more information about Microsoft antimalware technology?** For more information, visit the [Microsoft Malware Protection Center](https://www.microsoft.com/security/portal/) website.**Suggested Actions****Verify that the update is installed** Customers should verify that the latest version of the Microsoft Malware Protection Engine and definition updates are being actively downloaded and installed for their Microsoft antimalware products.For more information on how to verify the version number for the Microsoft Malware Protection Engine that your software is currently using, see the section, "Verifying Update Installation", in [Microsoft Knowledge Base Article 2510781](https://support.microsoft.com/kb/2510781).For affected software, verify that the Microsoft Malware Protection Engine version is 1.1.14405.2 or later.**If necessary, install the update** Administrators of enterprise antimalware deployments should ensure that their update management software is configured to automatically approve and distribute engine updates and new malware definitions. Enterprise administrators should also verify that the latest version of the Microsoft Malware Protection Engine and definition updates are being actively downloaded, approved and deployed in their environment.For end-users, the affected software provides built-in mechanisms for the automatic detection and deployment of this update. For these customers, the update will be applied within 48 hours of its availability. The exact time frame depends on the software used, Internet connection, and infrastructure configuration. End users that do not wish to wait can manually update their antimalware software.For more information on how to manually update the Microsoft Malware Protection Engine and malware definitions, refer to [Microsoft Knowledge Base Article 2510781](https://support.microsoft.com/kb/2510781).**Mitigations:**None **Workarounds:**None **Revision:**1.2    12/12/2017 08:00:00    Changed Microsoft Forefront Endpoint Protection to Microsoft System Center Endpoint Protection in the Affected Products table.1.1    12/08/2017 08:00:00    Added information to the Frequently Asked Questions.1.0    12/07/2017 08:00:00    Information published.  | Critical | Remote Code Execution |

## Affected Software

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

| **CVE-2017-11940** |
| --- |
| **Product** | **KB Article** | **Severity** | **Impact** | **Supersedence** | **CVSS Score Set** | **Restart Required** |
| Microsoft Security Essentials |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Intune Endpoint Protection |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Microsoft Exchange Server 2013 |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Microsoft Exchange Server 2016 |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Microsoft Forefront Endpoint Protection 2010 |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Microsoft System Center Endpoint Protection |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 7 for 32-bit Systems Service Pack 1 |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 7 for x64-based Systems Service Pack 1 |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 8.1 for 32-bit systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 8.1 for x64-based systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows RT 8.1 |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1511 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1511 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows Server 2016 |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1607 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1607 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows Server 2016 (Server Core installation) |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1703 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1703 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1709 for 32-bit Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |
| Windows Defender on Windows 10 Version 1709 for x64-based Systems |  | Critical | Remote Code Execution |  | Base: N/ATemporal: N/AVector: N/A |  |

**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