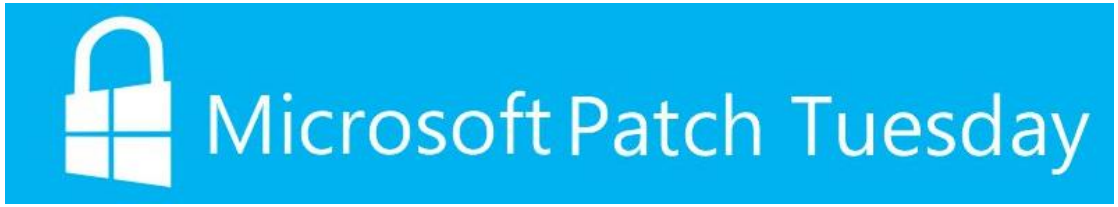
微软发布 11 月补丁修复 53 个安全问题

安全威胁通告



发布时间：2017 年 11 月 14 日

综述

微软于周二发布了 11 月安全更新补丁，修复了 53 个从简单的欺骗攻击到远程执行代码的安全问题，产品涉及.NET Framework、Adobe Flash Player、ASP .NET、ASP.NET、Device Guard、Internet Explorer、Microsoft Browsers、Microsoft Edge、Microsoft Graphics Component、Microsoft Office、Microsoft Scripting Engine、Microsoft Windows Search Component、None、Windows Kernel、Windows Kernel-Mode Drivers 以及 Windows Media Player。

相关信息如下（红色部分威胁相对比较高）：

产品	CVE 编号	CVE 标题
.NET Framework	CVE-2017-11770	.NET CORE 拒绝服务漏洞
Adobe Flash Player	ADV170019	November 2017 Flash 安全更新 s
ASP .NET	CVE-2017-8700	ASP.NET Core 信息泄露漏洞
ASP.NET	CVE-2017-11879	ASP.NET Core 提权漏洞
Device Guard	CVE-2017-11830	Device Guard 安全功能绕过漏洞
Internet Explorer	CVE-2017-11856	Internet Explorer 内存破坏漏洞
Internet Explorer	CVE-2017-11848	Internet Explorer 信息泄露漏洞

Internet Explorer	CVE-2017-11855	Internet Explorer 内存破坏漏洞
Microsoft Browsers	CVE-2017-11827	Microsoft Browser 内存破坏漏洞
Microsoft Edge	CVE-2017-11803	Microsoft Edge 信息泄露漏洞
Microsoft Edge	CVE-2017-11833	Microsoft Edge 信息泄露漏洞
Microsoft Edge	CVE-2017-11844	Microsoft Edge 信息泄露漏洞
Microsoft Edge	CVE-2017-11845	Microsoft Edge 内存破坏漏洞
Microsoft Edge	CVE-2017-11863	Microsoft Edge 安全功能绕过漏洞
Microsoft Edge	CVE-2017-11872	Microsoft Edge 安全功能绕过漏洞

Microsoft Edge	CVE-2017-11874	Microsoft Edge 安全功能绕过漏洞
Microsoft Graphics Component	CVE-2017-11832	Windows EOT Font Engine 信息泄露漏洞
Microsoft Graphics Component	CVE-2017-11851	Windows Kernel 信息泄露漏洞
Microsoft Graphics Component	CVE-2017-11835	Windows EOT Font Engine 信息泄露漏洞
Microsoft Graphics Component	CVE-2017-11850	Microsoft Graphics Component 信息泄露漏洞
Microsoft Graphics Component	CVE-2017-11852	Windows GDI 信息泄露漏洞
Microsoft Office	CVE-2017-11876	Microsoft Project Server 特权提升漏洞
Microsoft Office	CVE-2017-11877	Microsoft Excel 安全功能绕过漏洞

Microsoft Office	CVE-2017-11878	Microsoft Excel 内存破坏漏洞
Microsoft Office	ADV170020	Microsoft Office Defense in Depth Update
Microsoft Office	CVE-2017-11884	Microsoft Office 内存破坏漏洞
Microsoft Office	CVE-2017-11854	Microsoft Word 内存破坏漏洞
Microsoft Office	CVE-2017-11882	Microsoft Office 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11791	Scripting Engine 信息泄露漏洞
Microsoft Scripting Engine	CVE-2017-11837	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11839	Scripting Engine 内存破坏漏洞

Microsoft Scripting Engine	CVE-2017-11841	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11861	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11862	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11870	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11873	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11834	Scripting Engine 信息泄露漏洞
Microsoft Scripting Engine	CVE-2017-11836	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11838	Scripting Engine 内存破坏漏洞

Microsoft Scripting Engine	CVE-2017-11840	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11843	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11846	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11866	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11858	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11869	Scripting Engine 内存破坏漏洞
Microsoft Scripting Engine	CVE-2017-11871	Scripting Engine 内存破坏漏洞
Microsoft Windows Search Component	CVE-2017-11788	Windows Search 拒绝服务漏洞

None	CVE-2017-11883	ASP.NET Core Denial Of Service Vulnerability
Windows Kernel	CVE-2017-11831	Windows 信息泄露漏洞
Windows Kernel	CVE-2017-11847	Windows Kernel 特权提升漏洞
Windows Kernel	CVE-2017-11880	Windows 信息泄露漏洞
Windows Kernel-Mode Drivers	CVE-2017-11842	Windows Kernel 信息泄露漏洞
Windows Kernel-Mode Drivers	CVE-2017-11849	Windows Kernel 信息泄露漏洞
Windows Kernel-Mode Drivers	CVE-2017-11853	Windows Kernel 信息泄露漏洞
Windows Media Player	CVE-2017-11768	Windows Media Player 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

ADV170019 - November 2017 Flash Security Updates

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV170019 MITRE NVD	**CVE Title:** November 2017 Flash Security Updates **Description:** This security update addresses the following vulnerability, which is described in Adobe Security Bulletin APSB17-33: CVE-2017-3112, CVE-2017-3114, CVE-2017-11213, CVE-2017-11215, CVE-2017-11225. **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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: Workaround refers to a setting or configuration change that would help block known attack vectors before you apply the update. • **Prevent Adobe Flash Player from running** You can disable attempts to instantiate Adobe Flash Player in Internet Explorer and other applications that honor the kill bit feature, such as Office 2007 and Office 2010, by setting the kill bit for the control in the registry. **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. To set the kill bit for the control in the registry, perform the following steps: 1. Paste the following into a text file and save it with the .reg file extension. Copy		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Windows Registry Editor Version 5.00 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] "Compatibility Flags"=dword:00000400 [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] "Compatibility Flags"=dword:00000400 2. Double-click the .reg file to apply it to an individual system. You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, Group Policy collection. **Note** You must restart Internet Explorer for your changes to take effect. **Impact of workaround**. There is no impact as long as the object is not intended to be used in Internet Explorer.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	How to undo the workaround. Delete the registry keys that were added in implementing this workaround. • **Prevent Adobe Flash Player from running in Internet Explorer through Group Policy** **Note** The Group Policy MMC snap-in can be used to set policy for a machine, for an organizational unit, or for an entire domain. For more information about Group Policy, visit the following Microsoft Web sites: Group Policy Overview What is Group Policy Object Editor? Core Group Policy tools and settings To disable Adobe Flash Player in Internet Explorer through Group Policy, perform the following steps: **Note** This workaround does not prevent Flash from being invoked from other applications, such as Microsoft Office 2007 or Microsoft Office 2010.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1. Open the Group Policy Management Console and configure the console to work with the appropriate Group Policy object, such as local machine, OU, or domain GPO. 2. Navigate to the following node: **Administrative Templates** -> **Windows Components** -> **Internet Explorer** -> **Security Features** -> **Add-on Management** 3. Double-click **Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects**. 4. Change the setting to **Enabled**. 5. Click **Apply** and then click **OK** to return to the Group Policy Management Console. 6. Refresh Group Policy on all systems or wait for the next scheduled Group Policy refresh interval for the settings to take effect. • **Prevent Adobe Flash Player from running in Office 2010 on affected systems**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Note This workaround does not prevent Adobe Flash Player from running in Internet Explorer. **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. For detailed steps that you can use to prevent a control from running in Internet Explorer, see Microsoft Knowledge Base Article 240797. Follow the steps in the article to create a Compatibility Flags value in the registry to prevent a COM object from being instantiated in Internet Explorer. To disable Adobe Flash Player in Office 2010 only, set the kill bit for the ActiveX control for Adobe Flash Player in the registry using the following steps: 1. Create a text file named Disable_Flash.reg with the following contents: Copy Windows Registry Editor Version 5.00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Common\COM\Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] "Compatibility Flags"=dword:00000400 2. Double-click the .reg file to apply it to an individual system. 3. **Note** You must restart Internet Explorer for your changes to take effect. You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, Group Policy collection. • **Prevent ActiveX controls from running in Office 2007 and Office 2010** To disable all ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, including Adobe Flash Player in Internet Explorer, perform the following steps: 1. Click **File**, click **Options**, click **Trust Center**, and then click **Trust Center Settings**. 2. Click **ActiveX Settings** in the left-hand pane, and then select **Disable all controls without notifications**.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	3. Click **OK** to save your settings. **Impact of workaround.** Office documents that use embedded ActiveX controls may not display as intended. **How to undo the workaround.** To re-enable ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, perform the following steps: 4. Click **File**, click **Options**, click **Trust Center**, and then click **Trust Center Settings**. 5. Click **ActiveX Settings** in the left-hand pane, and then deselect **Disable all controls without notifications**. 6. Click **OK** to save your settings. • **Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	You can help protect against exploitation of these vulnerabilities by changing your settings for the Internet security zone to block ActiveX controls and Active Scripting. You can do this by setting your browser security to High. To raise the browsing security level in Internet Explorer, perform the following steps: 1. On the Internet Explorer **Tools** menu, click **Internet Options**. 2. In the **Internet Options** dialog box, click the **Security** tab, and then click **Internet**. 3. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 4. Click **Local intranet**. 5. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 6. Click **OK** to accept the changes and return to Internet Explorer. **Note** If no slider is visible, click **Default Level**, and then move the slider to **High**. **Note** Setting the level to High may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly even with the security setting set to High.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Impact of workaround. There are side effects to blocking ActiveX Controls and Active Scripting. Many websites on the Internet or an intranet use ActiveX or Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX Controls to provide menus, ordering forms, or even account statements. Blocking ActiveX Controls or Active Scripting is a global setting that affects all Internet and intranet sites. If you do not want to block ActiveX Controls or Active Scripting for such sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". • **Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone** You can help protect against exploitation of these vulnerabilities by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone. To do this, perform the following steps: 1. In Internet Explorer, click **Internet Options** on the **Tools** menu. 2. Click the **Security** tab. 3. Click **Internet**, and then click **Custom Level**.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	4. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 5. Click **Local intranet**, and then click **Custom Level**. 6. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 7. Click **OK** to return to Internet Explorer, and then click **OK** again. **Note** Disabling Active Scripting in the Internet and Local intranet security zones may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly. **Impact of workaround.** There are side effects to prompting before running Active Scripting. Many websites that are on the Internet or on an intranet use Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use Active Scripting to provide menus, ordering forms, or even account statements. Prompting before running Active Scripting is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you feel you trust the site that you are visiting, click **Yes** to run Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone".		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• **Add sites that you trust to the Internet Explorer Trusted sites zone** After you set Internet Explorer to require a prompt before it runs ActiveX controls and Active Scripting in the Internet zone and in the Local intranet zone, you can add sites that you trust to the Internet Explorer Trusted sites zone. This will allow you to continue to use trusted websites exactly as you do today, while helping to protect you from this attack on untrusted sites. We recommend that you add only sites that you trust to the Trusted sites zone. To do this, perform the following steps: 1. In Internet Explorer, click **Tools**, click **Internet Options**, and then click the **Security** tab. 2. In the **Select a web content zone to specify its current security settings** box, click **Trusted Sites**, and then click **Sites**. 3. If you want to add sites that do not require an encrypted channel, click to clear the **Require server verification (https:) for all sites in this zone** check box. 4. In the **Add this website to the zone** box, type the URL of a site that you trust, and then click **Add**.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	5. Repeat these steps for each site that you want to add to the zone. 6. Click **OK** two times to accept the changes and return to Internet Explorer. **Note** Add any sites that you trust not to take malicious action on your system. Two sites in particular that you may want to add are ***.windowsupdate.microsoft.com** and ***.update.microsoft.com**. These are the sites that will host the update, and they require an ActiveX control to install the update. **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

ADV170019						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

ADV170019						
Adobe Flash Player on Windows Server 2012	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for 32-bit systems	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for x64-based systems	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2012 R2	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows RT 8.1	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 for 32-bit Systems	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal:	Yes

ADV170019						
					N/A Vector: N/A	
Adobe Flash Player on Windows 10 for x64-based Systems	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1511 for x64-based Systems	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1511 for 32-bit Systems	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2016	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV170019						
Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for 32-bit Systems	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for 64-based Systems	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server, version 1709 (Server Core Installation)	4048951 Security Update	Critical	Remote Code Execution	4049179	Base: N/A Temporal:	Yes

ADV170019						
					N/A Vector: N/A	

ADV170020 - Microsoft Office Defense in Depth Update

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV170020 MITRE NVD	**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. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.	None	Defense in Depth

Affected Software

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

ADV170020						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Word 2007 Service Pack 3	4011266 Security Update	None	Defense in Depth	3213648	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011270 Security Update	None	Defense in Depth	3213630	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4011270 Security Update	None	Defense in Depth	3213630	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011268 Security Update	None	Defense in Depth	3213627	Base: N/A Temporal: N/A Vector: N/A	Maybe

ADV170020						
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011268 Security Update	None	Defense in Depth	3213627	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps 2010 Service Pack 2	4011271 Security Update	None	Defense in Depth	4011194	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4011250 Security Update	None	Defense in Depth	4011232	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4011250 Security Update	None	Defense in Depth	4011232	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 RT Service Pack 1	4011250 Security Update	None	Defense in Depth	4011232	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps Server 2013 Service Pack 1	4011247 Security Update	None	Defense in Depth	4011231	Base: N/A Temporal:	Maybe

ADV170020						
					N/A Vector: N/A	
Microsoft Word 2016 for Mac	Release Notes Security Update	None	Defense in Depth	4011231	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Word 2016 (32-bit edition)	4011242 Security Update	None	Defense in Depth	4011222	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (64-bit edition)	4011242 Security Update	None	Defense in Depth	4011222	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4011244 Security Update	None	Defense in Depth	4011217	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Word Viewer	4011264 Security Update	None	Defense in Depth	4011236	Base: N/A Temporal: N/A Vector: N/A	Maybe

ADV170020						
Microsoft Office Compatibility Pack Service Pack 3	4011265 Security Update	None	Defense in Depth	3213647	Base: N/A Temporal: N/A Vector: N/A	Maybe
Word Automation Services on Microsoft SharePoint Server 2010 Service Pack 2	4011267 Security Update	None	Defense in Depth	3213623	Base: N/A Temporal: N/A Vector: N/A	Maybe
Word Automation Services on Microsoft SharePoint Server 2013 Service Pack 1	4011245 Security Update	None	Defense in Depth	4011068	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11768 - Windows Media Player Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-	**CVE Title:** Windows Media Player Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
11768 MITRE NVD	An information vulnerability exists when Windows Media Player improperly discloses file information. Successful exploitation of the vulnerability could allow the attacker to test for the presence of files on disk. To exploit the vulnerability, an attacker would have to log onto an affected system and run a specially crafted application. The update addresses the vulnerability by changing the way Windows Media Player discloses file information. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11768						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows 7 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes

CVE-2017-11768						
(Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows Server 2012	4048959 Monthly Rollup 4048962 Security Only	Important	Information Disclosure	4041690	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes

CVE-2017-11768						
Windows Server 2012 (Server Core installation)	4048959 Monthly Rollup 4048962 Security Only	Important	Information Disclosure	4041690	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows 8.1 for 32-bit systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows 8.1 for x64-based systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes

CVE-2017-11768						
Windows Server 2012 R2	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows RT 8.1	4048958 Monthly Rollup	Important	Information Disclosure	4041693	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows Server 2012 R2 (Server Core installation)	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows 10 for 32-bit Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes

CVE-2017-11768						
Windows 10 for x64-based Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows Server 2016	4048953 Security Update	Important	Information Disclosure	4041691	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows 10 Version 1607	4048953 Security	Important	Information Disclosure	4041691	Base: 2.5 Temporal: 2.2	Yes

CVE-2017-11768						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	
Windows Server 2016 (Server Core installation)	4048953 Security Update	Important	Information Disclosure	4041691	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes
Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes

CVE-2017-11768						
Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Important	Information Disclosure	4042198	Base: 2.5 Temporal: 2.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O	Yes

CVE-2017-11770 - .NET CORE Denial Of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11770 MITRE NVD	**CVE Title:** .NET CORE Denial Of Service Vulnerability **Description:** A denial of service vulnerability exists when .NET Core improperly handles parsing certificate data. An attacker who successfully exploited this vulnerability could cause a denial of service against a .NET Core web application. The vulnerability can be exploited remotely, without authentication. A remote unauthenticated attacker could exploit this vulnerability by providing a specially crafted certificate to the .NET Core application.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by correcting how the .NET Core web application handles parsing certificate data. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11770						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11770						
.NET Core 1.0	Commit Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Yes
.NET Core 1.1	Commit Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Yes
.NET Core 2.0	Commit Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-11788 - Windows Search Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11788 MITR	**CVE Title:** Windows Search Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Windows Search improperly handles objects in memory. An attacker who successfully exploited the vulnerability could cause a remote denial of service against a system.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
E NVD	To exploit the vulnerability, the attacker could send specially crafted messages to the Windows Search service. Additionally, in an enterprise scenario, a remote unauthenticated attacker could remotely trigger the vulnerability through a Server Message Block (SMB) connection. The security update addresses the vulnerability by correcting how Windows Search handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** **Disable WSearch service** Interactive workaround deployment steps 1. Click **Start**, click **Run**, type "regedit" (without the quotation marks), and then click **OK**. 2. Expand HKEY_LOCAL_MACHINE 3. Expand System, then CurrentControlSet, then Services 4. Click on **WSearch**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	5. Click the **File** menu and select Export. 6. In the **Export Registry File** dialog type â€œWSearch_configuration_backup.regâ€☐ and press **Save**. 7. Double-click the value named **Start** and change the **Value** data field to 4 8. Click **OK** 9. Run the following command at a command prompt running as an administrator: **sc stop WSearch** Impact of workaround The Windows Search functionality will not be available to applications that use it for searches. How do undo the workaround 1. Click **Start** , click **Run** , type "regedit " (without the quotation marks), and then click **OK**. 2. Click the **File** menu and select Import. 3. In the **Import Registry File** dialog select â€œWSearch_configuration_backup.regâ€☐ and press **Open**. Managed workaround deployment steps		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1. First a backup copy of the registry keys can be made from a managed deployment script with the following command: **regedit /e WSearch_configuration_backup.reg HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WSearch** 2. Next save the following to a file with a .REG extension (e.g. Disable_WSearch.reg) **Windows Registry Editor Version 5.00** **[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WSearch]** **"Start"=dword:00000004** 3. Run the registry script created in step 2 on the target machine with the following command: **regedit /s Disable_WSearch .reg** 4. Run the following command at a command prompt running as an administrator: **sc stop WSearch** Impact of workaround The Windows Search functionality will not be available to applications that use it for searches. How to undo the workaround		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Restore the original state by running the following command: **regedit /s WSearch_configuration_backup.reg** **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11788						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security	Important	Denial of Service	4041681	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11788						
	Only					
Windows 7 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Denial of Service	4041681	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4048957 Monthly Rollup 4048960 Security Only	Important	Denial of Service	4041681	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based	4048957 Monthly Rollup 4048960 Security	Important	Denial of Service	4041681	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11788						
Systems Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Denial of Service	4041681	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4047211 Security Update	Important	Denial of Service	4041681	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4048959 Monthly Rollup 4048962 Security	Important	Denial of Service	4041690	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11788						
	Only					
Windows Server 2012 (Server Core installation)	4048959 Monthly Rollup 4048962 Security Only	Important	Denial of Service	4041690	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4048958 Monthly Rollup 4048961 Security Only	Important	Denial of Service	4041693	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4048958 Monthly Rollup 4048961 Security Only	Important	Denial of Service	4041693	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11788						
Windows Server 2012 R2	4048958 Monthly Rollup 4048961 Security Only	Important	Denial of Service	4041693	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4048958 Monthly Rollup	Important	Denial of Service	4041693	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4048958 Monthly Rollup 4048961 Security Only	Important	Denial of Service	4041693	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4048956 Security Update	Important	Denial of Service	4042895	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11788						
Windows 10 for x64-based Systems	4048956 Security Update	Important	Denial of Service	4042895	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Important	Denial of Service	4041689	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Denial of Service	4041689	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4048953 Security Update	Important	Denial of Service	4041691	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Denial of Service	4041691	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11788						
Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Denial of Service	4041691	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4048953 Security Update	Important	Denial of Service	4041691	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Denial of Service	4041676	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Denial of Service	4041676	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server	4048955 Security Update	Important	Denial of Service	4042198	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11788						
Core Installation)						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4047211 Security Update	Important	Denial of Service	4042198	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4047211 Security Update	Important	Denial of Service	4042198	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4047211 Security Update	Important	Denial of Service	4042198	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11788						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4047211 Security Update	Important	Denial of Service	4042198	Base: 5.9 Temporal: 5.3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11791 - Scripting Engine Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11791 MITRE NVD	**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.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11791						
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	4047206 IE Cumulative	Low	Information Disclosure	4040685	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server	4047206 IE Cumulative	Low	Information Disclosure	4040685	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11791						
2008 for x64-based Systems Service Pack 2						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Important	Information Disclosure	4041681	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Important	Information Disclosure	4041681	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11791						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Low	Information Disclosure	4041681	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4047206 IE Cumulative 4048958 Monthly Rollup	Important	Information Disclosure	4041693	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for	4047206 IE Cumulative 4048958 Monthly	Important	Information Disclosure	4041693	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11791						
x64-based systems	Rollup					
Internet Explorer 11 on Windows Server 2012 R2	4047206 IE Cumulative 4048958 Monthly Rollup	Low	Information Disclosure	4041693	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4048958 Monthly Rollup	Important	Information Disclosure	4041693	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11791						
Internet Explorer 11 on Windows 10 for x64-based Systems	4042895 Security Update	Important	Information Disclosure	4038781	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11791						
Internet Explorer 11 on Windows Server 2016	4048953 Security Update	Low	Information Disclosure	4041691	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11791						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11791						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Low	Information Disclosure	4042198	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes

CVE-2017-11791						
Internet Explorer 10 on Windows Server 2012	4048959 Monthly Rollup 4047206 IE Cumulative	Low	Information Disclosure	4040685	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for 32-bit Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2017-11791						
1511 for x64-based Systems					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	
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4048953 Security Update	Low	Information Disclosure	4041691	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11791						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11791						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server, version 1709 (Server Core	4048955 Security Update	Low	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11791						
Installation)						
ChakraCore	Commit Security Only	Important	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11803 - Microsoft Edge Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11803 MITRE NVD	**CVE Title:** Microsoft Edge Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11803						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11803						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Low	Information Disclosure	4042198	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11827 - Microsoft Browser Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11827 MITRE NVD	**CVE Title:** Microsoft Browser Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory. The vulnerability could corrupt memory in a way that could allow 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, 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 that is designed to exploit the vulnerability through Microsoft browsers, 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. 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 via an enticement in email or instant message, or by getting them to open an email attachment.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how Microsoft browsers handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11827						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11827						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Important	Remote Code Execution	4041681	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Important	Remote Code Execution	4041681	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2	4047206 IE Cumulative 4048957 Monthly	Low	Remote Code Execution	4041681	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11827						
for x64-based Systems Service Pack 1	Rollup					
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4047206 IE Cumulative 4048958 Monthly Rollup	Important	Remote Code Execution	4041693	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4047206 IE Cumulative 4048958 Monthly Rollup	Important	Remote Code Execution	4041693	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4047206 IE Cumulative 4048958	Low	Remote Code Execution	4041693	Base: 6.4 Temporal: 5.8 Vector:	Yes

CVE-2017-11827						
Server 2012 R2	Monthly Rollup				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	
Internet Explorer 11 on Windows RT 8.1	4048958 Monthly Rollup	Important	Remote Code Execution	4041693	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4048956 Security Update	Important	Remote Code Execution	4042895	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4048956 Security Update	Important	Remote Code Execution	4042895	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11	4048952 Security	Important	Remote Code	4041689	Base: 7.5 Temporal: 6.7	Yes

CVE-2017-11827						
on Windows 10 Version 1511 for x64-based Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Remote Code Execution	4041689	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4048953 Security Update	Low	Remote Code Execution	4041691	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4048953 Security	Important	Remote Code	4041691	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2017-11827						
Windows 10 Version 1607 for 32-bit Systems	Update		Execution		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	
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Remote Code Execution	4041691	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Remote Code Execution	4041676	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11	4048954 Security	Important	Remote Code	4041676	Base: 7.5 Temporal: 6.7	Yes

CVE-2017-11827						
on Windows 10 Version 1703 for x64-based Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Remote Code Execution	4042198	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Remote Code Execution	4042198	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11827						
Internet Explorer 11 on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Low	Remote Code Execution	4042198	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 10 on Windows Server 2012	4048959 Monthly Rollup 4047206 IE Cumulative	Low	Remote Code Execution	4040685	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for 32-bit Systems	4048956 Security Update	Important	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11827						
Microsoft Edge on Windows 10 for x64-based Systems	4048956 Security Update	Important	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Important	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11830 - Device Guard Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11830 MITRE NVD	**CVE Title:** Device Guard 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	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11830						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4048956 Security Update	Important	Security Feature Bypass	4042895	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4048956 Security Update	Important	Security Feature Bypass	4042895	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11830						
Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Important	Security Feature Bypass	4041689	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Security Feature Bypass	4041689	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016	4048953 Security Update	Important	Security Feature Bypass	4041691	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Security Feature Bypass	4041691	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Security Feature Bypass	4041691	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11830						
Windows Server 2016 (Server Core installation)	4048953 Security Update	Important	Security Feature Bypass	4041691	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Security Feature Bypass	4041676	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Security Feature Bypass	4041676	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Security Feature Bypass	4042198	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Security Feature Bypass	4042198	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2017-11830						
Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Important	Security Feature Bypass	4042198	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O	Yes

CVE-2017-11831 - Windows Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11831 MITRE NVD	**CVE Title:** Windows Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel initializes memory.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11831						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11831						
Windows 7 for 32-bit Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems	4048957 Monthly Rollup 404896	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11831						
Service Pack 1 (Server Core installation)	0 Security Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11831						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4046184 Security Update	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4048959 Monthly Rollup 4048962 Security Only	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server	4048959 Monthly Rollup	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11831						
Core installation)	4048962 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11831						
Windows Server 2012 R2	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4048958 Monthly Rollup	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11831						
Windows 10 for 32-bit Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4048953 Security	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11831						
	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11831						
Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

CVE-2017-11831						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4046184 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4046184 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4046184 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11831						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4046184 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11832 - Windows EOT Font Engine Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11832	**CVE Title:** Windows EOT Font Engine Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An information disclosure vulnerability exists in the way that the Microsoft Windows Embedded OpenType (EOT) font engine parses specially crafted embedded fonts. An attacker who successfully exploited this vulnerability could potentially read data that was not intended to be disclosed. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. To exploit this vulnerability, an attacker would have to log on to an affected system and open a document containing specially crafted fonts. The security update addresses the vulnerability by correcting how the Windows EOT font engine handles embedded fonts. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11832						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11832						
	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11832						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4048968 Security Update	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4048959 Monthly	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11832						
	Rollup 4048962 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4048959 Monthly Rollup 4048962 Security Only	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4048968 Security Update	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11832						
Windows Server 2008 for 32-bit Systems Service Pack 2	4048968 Security Update	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4048968 Security Update	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core	4048968 Security Update	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11832						
installation)						

CVE-2017-11833 - Microsoft Edge Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11833 MITRE NVD	**CVE Title:** Microsoft Edge Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests. An attacker who successfully exploited this vulnerability could determine the origin of all webpages in the affected browser. In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability. Additionally, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could be used to exploit the vulnerability. However, in all cases an attacker would have no way to force users to view attacker-controlled content. Instead, an attacker would have to convince users to take action. For example, an attacker could trick users into clicking a link that takes them to the attacker's site.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Microsoft Edge handles cross-origin requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11833						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11833						
Microsoft Edge on Windows 10 for 32-bit Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11833						
32-bit Systems						
Microsoft Edge on Windows Server 2016	4048953 Security Update	Low	Information Disclosure	4041691	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11833						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11833						
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Low	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11834 - Scripting Engine Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11834 MITRE NVD	**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 Internet Explorer. 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:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11834						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows	4047206 IE Cumulativ	Low	Information Disclosure	4040685	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2017-11834						
Server 2008 for 32-bit Systems Service Pack 2	e				CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4047206 IE Cumulative	Low	Information Disclosure	4040685	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for 32-bit Systems	4047206 IE Cumulative 4048957 Monthly	Important	Information Disclosure	4041681	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11834						
Service Pack 1	Rollup					
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Important	Information Disclosure	4041681	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/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	4047206 IE Cumulative 4048957 Monthly Rollup	Low	Information Disclosure	4041681	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11834						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4047206 IE Cumulative 4048958 Monthly Rollup	Important	Information Disclosure	4041693	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4047206 IE Cumulative 4048958 Monthly Rollup	Important	Information Disclosure	4041693	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4047206 IE Cumulative 4048958 Monthly	Low	Information Disclosure	4041693	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11834						
	Rollup					
Internet Explorer 11 on Windows RT 8.1	4048958 Monthly Rollup	Important	Information Disclosure	4041693	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11834						
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4048953 Security Update	Low	Information Disclosure	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11834						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for	4048954 Security Update	Important	Information Disclosure	4041676	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11834						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4048955 Security Update	Important	Information Disclosure	4042198	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11834						
1709 for 64-based Systems						
Internet Explorer 11 on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Low	Information Disclosure	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 10 on Windows Server 2012	4048959 Monthly Rollup 4047206 IE Cumulative	Low	Information Disclosure	4040685	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11835 - Windows EOT Font Engine Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11835 MITRE NVD	**CVE Title:** Windows EOT Font Engine Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that the Microsoft Windows Embedded OpenType (EOT) font engine parses specially crafted embedded fonts. An attacker who successfully exploited this vulnerability could potentially read data that was not intended to be disclosed. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. To exploit this vulnerability, an attacker would have to log on to an affected system and open a document containing specially crafted fonts. The security update addresses the vulnerability by correcting how the Windows EOT font engine handles embedded fonts. **FAQ:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11835						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4048957 Monthly Rollup	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11835						
Service Pack 1	4048960 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 7 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11835						
installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for	4048968 Security	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11835						
32-bit Systems Service Pack 2 (Server Core installation)	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4048968 Security Update	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4048968 Security Update	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11835						
Windows Server 2008 for x64-based Systems Service Pack 2	4048968 Security Update	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4048968 Security Update	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11836 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11836 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11836						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows	4048956 Security	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11836						
10 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 for x64-based Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11836						
Microsoft Edge on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/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	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11836						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11836						
Microsoft Edge on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11837 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
11837 MITRE NVD	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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11837						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit	4047206 IE Cumulative 4048957 Monthly	Critical	Remote Code Execution	4041681	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11837						
Systems Service Pack 1	Rollup					
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Critical	Remote Code Execution	4041681	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Moderate	Remote Code Execution	4041681	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11837						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4047206 IE Cumulative 4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4047206 IE Cumulative 4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4047206 IE Cumulative 4048958 Monthly Rollup	Moderate	Remote Code Execution	4041693	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11	4048958 Monthly	Critical	Remote Code	4041693	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11837						
on Windows RT 8.1	Rollup		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 for 32-bit Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11837						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11837						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11837						
1703 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2017-11837						
Server, version 1709 (Server Core Installation)						
Microsoft Edge on Windows 10 for 32-bit Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11837						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/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	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4048953 Security	Critical	Remote Code	4041691	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11837						
Windows 10 Version 1607 for x64-based Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2017-11837						
1709 for 32-bit Systems					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	
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
ChakraCore	Commit Security	Critical	Remote Code	4042198	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2017-11837						
	Only		Execution		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	

CVE-2017-11838 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11838 MITRE NVD	**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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11838						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Critical	Remote Code Execution	4041681	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Critical	Remote Code Execution	4041681	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on	4047206 IE Cumulative	Moderate	Remote Code	4041681	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-11838						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4048957 Monthly Rollup		Execution			
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4047206 IE Cumulative 4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4047206 IE Cumulative 4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-11838						
Internet Explorer 11 on Windows Server 2012 R2	4047206 IE Cumulative 4048958 Monthly Rollup	Moderate	Remote Code Execution	4041693	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows RT 8.1	4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 for x64-	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-11838						
based Systems						
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-11838						
Server 2016						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-11838						
1703 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-11838						
10 Version 1709 for 64-based Systems						
Internet Explorer 11 on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: N/A Temporal: N/A Vector: N/A	Yes
Microsoft Edge on Windows 10 for 32-bit Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4048956 Security	Critical	Remote Code	4042895	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2017-11838						
10 for x64-based Systems	Update		Execution		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	
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11838						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4048954 Security	Critical	Remote Code	4041676	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11838						
Windows 10 Version 1703 for x64-based Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server,	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 3.1 Temporal: 2.8 Vector:	Yes

CVE-2017-11838						
version 1709 (Server Core Installation)					CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11839 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11839	**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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11839						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11839						
based Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4048953 Security	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11839						
10 Version 1607 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11839						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server, version 1709 (Server	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2017-11839						
Core Installation)						

CVE-2017-11840 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11840 MITRE NVD	**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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11840						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4048952 Security	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11840						
10 Version 1511 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/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	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11840						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11840						
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11841 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11841 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11841						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows	4048956 Security	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11841						
10 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 for x64-based Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11841						
Microsoft Edge on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/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	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11841						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11841						
Microsoft Edge on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11842 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
11842 MITRE NVD	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel initializes memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11842						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4048959 Monthly Rollup 4048962 Security Only	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4048959 Monthly Rollup 4048962	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11842						
	Security Only					
Windows 8.1 for 32-bit systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11842						
Windows Server 2012 R2	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4048958 Monthly Rollup	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11842						
Windows 10 for 32-bit Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4048953 Security	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11842						
	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11842						
Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

CVE-2017-11843 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11843 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11843						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11843						
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4047206 IE Cumulative	Critical	Remote Code	4041681	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2017-11843						
Windows 7 for 32-bit Systems Service Pack 1	4048957 Monthly Rollup		Execution		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	
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Critical	Remote Code Execution	4041681	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems	4047206 IE Cumulative 4048957 Monthly Rollup	Moderate	Remote Code Execution	4041681	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11843						
Service Pack 1						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4047206 IE Cumulative 4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4047206 IE Cumulative 4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4047206 IE Cumulative 4048958 Monthly Rollup	Moderate	Remote Code Execution	4041693	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11843						
Internet Explorer 11 on Windows RT 8.1	4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11843						
1511 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11843						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11843						
1703 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2017-11843						
Server, version 1709 (Server Core Installation)						
Internet Explorer 10 on Windows Server 2012	4048959 Monthly Rollup 4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for 32-bit Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2017-11843						
based Systems					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	
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4048953 Security	Critical	Remote Code	4041691	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11843						
Windows 10 Version 1607 for 32-bit Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2017-11843						
1703 for x64-based Systems					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	
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server, version 1709	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2017-11843						
(Server Core Installation)						
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11844 - Microsoft Edge Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11844 MITRE NVD	**CVE Title:** Microsoft Edge Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.	Low	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11844						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11844						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server, version 1709 (Server Core	4048955 Security Update	Low	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11844						
Installation)						

CVE-2017-11845 - Microsoft Edge Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11845 MITRE NVD	**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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11845						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11846 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11846 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11846						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11846						
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4047206 IE Cumulative	Critical	Remote Code	4041681	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2017-11846						
Windows 7 for 32-bit Systems Service Pack 1	4048957 Monthly Rollup		Execution		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	
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Critical	Remote Code Execution	4041681	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems	4047206 IE Cumulative 4048957 Monthly Rollup	Moderate	Remote Code Execution	4041681	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11846						
Service Pack 1						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4047206 IE Cumulative 4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4047206 IE Cumulative 4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4047206 IE Cumulative 4048958 Monthly Rollup	Moderate	Remote Code Execution	4041693	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11846						
Internet Explorer 11 on Windows RT 8.1	4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11846						
1511 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11846						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11846						
1703 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2017-11846						
Server, version 1709 (Server Core Installation)						
Internet Explorer 10 on Windows Server 2012	4048959 Monthly Rollup 4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for 32-bit Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2017-11846						
based Systems					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	
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4048953 Security	Critical	Remote Code	4041691	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11846						
Windows 10 Version 1607 for 32-bit Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2017-11846						
1703 for x64-based Systems					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	
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server, version 1709	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2017-11846						
(Server Core Installation)						
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11847 - Windows Kernel Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11847 MITRE NVD	**CVE Title:** Windows Kernel Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system. The update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11847						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Elevation of Privilege	4041681	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Elevation of Privilege	4041681	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server	4048957 Monthly Rollup 4048960 Security Only	Important	Elevation of Privilege	4041681	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11847						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Elevation of Privilege	4041681	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Elevation of Privilege	4041681	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server	4048970 Security Update	Important	Elevation of Privilege	4042120	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11847						
Core installation)						
Windows Server 2012	4048959 Monthly Rollup 4048962 Security Only	Important	Elevation of Privilege	4041690	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4048959 Monthly Rollup 4048962 Security Only	Important	Elevation of Privilege	4041690	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4048958 Monthly Rollup 4048961 Security Only	Important	Elevation of Privilege	4041693	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11847						
Windows 8.1 for x64-based systems	4048958 Monthly Rollup 4048961 Security Only	Important	Elevation of Privilege	4041693	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4048958 Monthly Rollup 4048961 Security Only	Important	Elevation of Privilege	4041693	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4048958 Monthly Rollup	Important	Elevation of Privilege	4041693	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4048958 Monthly Rollup 4048961 Security	Important	Elevation of Privilege	4041693	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11847						
	Only					
Windows 10 for 32-bit Systems	4048956 Security Update	Important	Elevation of Privilege	4042895	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4048956 Security Update	Important	Elevation of Privilege	4042895	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Important	Elevation of Privilege	4041689	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Elevation of Privilege	4041689	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4048953 Security	Important	Elevation of Privilege	4041691	Base: 7 Temporal: 6.3	Yes

CVE-2017-11847						
	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Elevation of Privilege	4041691	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Elevation of Privilege	4041691	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4048953 Security Update	Important	Elevation of Privilege	4041691	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Elevation of Privilege	4041676	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11847						
Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Elevation of Privilege	4041676	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Important	Elevation of Privilege	4042198	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4048970 Security Update	Important	Elevation of Privilege	4042120	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4048970 Security Update	Important	Elevation of Privilege	4042120	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11847						
Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2	4048970 Security Update	Important	Elevation of Privilege	4042120	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4048970 Security Update	Important	Elevation of Privilege	4042120	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11848 - Internet Explorer Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11848 MITRE NVD	**CVE Title:** Internet Explorer Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Internet Explorer improperly handles page content, which could allow an attacker to detect the navigation of the user leaving a maliciously crafted page. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a specially crafted website. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by changing how page content is handled by Internet Explorer. **FAQ:** None **Mitigations:** None **Workarounds:**	Low	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11848						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems	4047206 IE Cumulative	Low	Information Disclosure	4040685	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11848						
Service Pack 2						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4047206 IE Cumulative	Low	Information Disclosure	4040685	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Moderate	Information Disclosure	4041681	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on	4047206 IE Cumulative	Moderate	Information Disclosure	4041681	Base: 4.3 Temporal: 3.9	Yes

CVE-2017-11848						
Windows 7 for x64-based Systems Service Pack 1	4048957 Monthly Rollup				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Low	Information Disclosure	4041681	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4047206 IE Cumulative 4048958 Monthly	Moderate	Information Disclosure	4041693	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11848						
	Rollup					
Internet Explorer 11 on Windows 8.1 for x64-based systems	4047206 IE Cumulative 4048958 Monthly Rollup	Moderate	Information Disclosure	4041693	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4047206 IE Cumulative 4048958 Monthly Rollup	Low	Information Disclosure	4041693	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4048958 Monthly Rollup	Moderate	Information Disclosure	4041693	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11848						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4048956 Security Update	Moderate	Information Disclosure	4042895	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4048956 Security Update	Moderate	Information Disclosure	4042895	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Moderate	Information Disclosure	4041689	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11848						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Moderate	Information Disclosure	4041689	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4048953 Security Update	Low	Information Disclosure	4041691	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Moderate	Information Disclosure	4041691	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11848						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Moderate	Information Disclosure	4041691	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Moderate	Information Disclosure	4041676	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for	4048954 Security Update	Moderate	Information Disclosure	4041676	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11848						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Moderate	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Moderate	Information Disclosure	4042198	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes
Internet Explorer 11 on Windows Server,	4048955 Security Update	Low	Information Disclosure	4042198	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-11848						
version 1709 (Server Core Installation)						
Internet Explorer 10 on Windows Server 2012	4048959 Monthly Rollup 4047206 IE Cumulative	Low	Information Disclosure	4040685	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11849 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
11849 MITRE NVD	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel initializes memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11849						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11849						
	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11849						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4048959 Monthly	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11849						
	Rollup 4048962 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4048959 Monthly Rollup 4048962 Security Only	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4048958 Monthly Rollup 4048961 Security	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11849						
	Only					
Windows 8.1 for x64-based systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4048958 Monthly	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11849						
	Rollup				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 R2 (Server Core installation)	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11849						
Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for	4048953 Security	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11849						
x64-based Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4048955 Security	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

CVE-2017-11849						
32-bit Systems	Update					
Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11849						
Windows Server 2008 for x64-based Systems Service Pack 2	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11850 - Microsoft Graphics Component Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11850 MITRE NVD	**CVE Title:** Microsoft Graphics Component Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Microsoft Windows Graphics Component improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The update addresses the vulnerability by correcting the way in which the Windows Graphics Component handles objects in memory. **FAQ:** None **Mitigations:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11850						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4048959 Monthly Rollup 4048962	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11850						
	Security Only					
Windows Server 2012 (Server Core installation)	4048959 Monthly Rollup 4048962 Security Only	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11850						
Windows 8.1 for x64-based systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4048958 Monthly Rollup	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11850						
Windows Server 2012 R2 (Server Core installation)	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4048952 Security	Important	Information Disclosure	4041689	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11850						
x64-based Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

CVE-2017-11850						
Windows Server 2016 (Server Core installation)	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

CVE-2017-11850						
Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

CVE-2017-11851 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
11851 MITRE NVD	A Win32k information disclosure vulnerability exists when the Windows GDI component improperly discloses kernel memory addresses. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11851						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11851						
	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11851						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4048959 Monthly Rollup	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11851						
	4048962 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4048959 Monthly Rollup 4048962 Security Only	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11851						
Windows 8.1 for x64-based systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4048958 Monthly Rollup	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11851						
Windows Server 2012 R2 (Server Core installation)	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4048952 Security	Important	Information Disclosure	4041689	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11851						
x64-based Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11851						
Windows Server 2016 (Server Core installation)	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

CVE-2017-11851						
Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11851						
Windows Server 2008 for 32-bit Systems Service Pack 2	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11851						
Core installation)						

CVE-2017-11852 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11852 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** A Win32k information disclosure vulnerability exists when the Windows GDI component improperly discloses kernel memory addresses. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system. The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11852						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11852						
Windows 7 for 32-bit Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems	4048957 Monthly Rollup 404896	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11852						
Service Pack 1 (Server Core installation)	0 Security Only					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11852						
	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11852						
Windows Server 2008 for 32-bit Systems Service Pack 2	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11852						
installation)						

CVE-2017-11853 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11853 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel initializes memory. **FAQ:** None	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11853						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4048957 Monthly Rollup 404896	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11853						
	0 Security Only					
Windows 7 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11853						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

CVE-2017-11853						
Service Pack 2 (Server Core installation)						
Windows Server 2012	4048959 Monthly Rollup 4048962 Security Only	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server 2012 (Server Core installation)	4048959 Monthly Rollup 4048962 Security Only	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

CVE-2017-11853						
Windows 8.1 for 32-bit systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4048958 Monthly Rollup 404896	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11853						
	1 Security Only					
Windows RT 8.1	4048958 Monthly Rollup	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11853						
Windows 10 for x64-based Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for	4048953 Security	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11853						
32-bit Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11853						
Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server 2008 for Itanium-Based	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

CVE-2017-11853						
Systems Service Pack 2						
Windows Server 2008 for 32-bit Systems Service Pack 2	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server 2008 for x64-based Systems Service	4048970 Security Update	Important	Information Disclosure	4042120	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

CVE-2017-11853						
Pack 2 (Server Core installation)						

CVE-2017-11854 - Microsoft Word Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11854 MITRE NVD	**CVE Title:** Microsoft Word Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office. 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) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11854						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Word 2007 Service Pack 3	4011266 Security Update	Important	Remote Code Execution	3213648	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011270 Security Update	Important	Remote Code Execution	3213630	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4011270 Security Update	Important	Remote Code Execution	3213630	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011268 Security Update	Important	Remote Code Execution	3213627	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11854						
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011268 Security Update	Important	Remote Code Execution	3213627	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Compatibility Pack Service Pack 3	4011265 Security Update	Important	Remote Code Execution	3213647	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11855 - Internet Explorer Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11855 MITRE NVD	**CVE Title:** Internet Explorer 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	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11855						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems	4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11855						
Service Pack 2						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Critical	Remote Code Execution	4041681	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4047206 IE Cumulative	Critical	Remote Code	4041681	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2017-11855						
Windows 7 for x64-based Systems Service Pack 1	4048957 Monthly Rollup		Execution		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	
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Moderate	Remote Code Execution	4041681	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4047206 IE Cumulative 4048958 Monthly	Critical	Remote Code Execution	4041693	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11855						
	Rollup					
Internet Explorer 11 on Windows 8.1 for x64-based systems	4047206 IE Cumulative 4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4047206 IE Cumulative 4048958 Monthly Rollup	Moderate	Remote Code Execution	4041693	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11	4048956 Security	Critical	Remote Code	4042895	Base: 7.5 Temporal: 6.7	Yes

CVE-2017-11855						
on Windows 10 for 32-bit Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 for x64-based Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2017-11855						
10 Version 1511 for 32-bit Systems					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	
Internet Explorer 11 on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11855						
1607 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2017-11855						
10 Version 1709 for 32-bit Systems					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	
Internet Explorer 11 on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11855						
Internet Explorer 10 on Windows Server 2012	4048959 Monthly Rollup 4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11856 - Internet Explorer Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11856 MITRE NVD	**CVE Title:** Internet Explorer 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11856						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Critical	Remote Code Execution	4041681	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11856						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Critical	Remote Code Execution	4041681	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Moderate	Remote Code Execution	4041681	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4047206 IE Cumulative	Critical	Remote Code	4041693	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2017-11856						
Windows 8.1 for 32-bit systems	4048958 Monthly Rollup		Execution		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	
Internet Explorer 11 on Windows 8.1 for x64-based systems	4047206 IE Cumulative 4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4047206 IE Cumulative 4048958 Monthly Rollup	Moderate	Remote Code Execution	4041693	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11856						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11	4048952 Security	Critical	Remote Code	4041689	Base: 7.5 Temporal: 6.7	Yes

CVE-2017-11856						
on Windows 10 Version 1511 for 32-bit Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4048953 Security	Critical	Remote Code	4041691	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2017-11856						
Windows 10 Version 1607 for x64-based Systems	Update		Execution		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	
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11	4048955 Security	Critical	Remote Code	4042198	Base: 7.5 Temporal: 6.7	Yes

CVE-2017-11856						
on Windows 10 Version 1709 for 32-bit Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server, version 1709 (Server Core	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11856						
Installation)						

CVE-2017-11858 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11858 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory. The vulnerability could corrupt memory in a way that could allow 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, 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 that is designed to exploit the vulnerability through Microsoft browsers, 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 via an enticement in email or instant message, or by getting them to open an email attachment. The security update addresses the vulnerability by modifying how Microsoft browsers handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11858						
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	4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11858						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Critical	Remote Code Execution	4041681	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Critical	Remote Code Execution	4041681	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2	4047206 IE Cumulative 4048957 Monthly	Moderate	Remote Code Execution	4041681	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11858						
for x64-based Systems Service Pack 1	Rollup					
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4047206 IE Cumulative 4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4047206 IE Cumulative 4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4047206 IE Cumulative 4048958	Moderate	Remote Code Execution	4041693	Base: 6.4 Temporal: 5.8 Vector:	Yes

CVE-2017-11858						
Server 2012 R2	Monthly Rollup				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	
Internet Explorer 11 on Windows RT 8.1	4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11	4048952 Security	Critical	Remote Code	4041689	Base: 7.5 Temporal: 6.7	Yes

CVE-2017-11858						
on Windows 10 Version 1511 for x64-based Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4048953 Security	Critical	Remote Code	4041691	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2017-11858						
Windows 10 Version 1607 for 32-bit Systems	Update		Execution		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	
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11	4048954 Security	Critical	Remote Code	4041676	Base: 7.5 Temporal: 6.7	Yes

CVE-2017-11858						
on Windows 10 Version 1703 for x64-based Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11858						
Internet Explorer 11 on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 10 on Windows Server 2012	4048959 Monthly Rollup 4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for 32-bit Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11858						
Microsoft Edge on Windows 10 for x64-based Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4048953 Security	Moderate	Remote Code	4041691	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11858						
Server 2016	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11858						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4048955 Security	Moderate	Remote Code	4042198	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11858						
Windows Server, version 1709 (Server Core Installation)	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11861 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11861	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11861						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11861						
1607 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11861						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server, version 1709 (Server	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11861						
Core Installation)						
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11862 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11862 MITRE NVD	**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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11862						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11862						
Microsoft Edge on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11863 - Microsoft Edge Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-	**CVE Title:** Microsoft Edge Security Feature Bypass Vulnerability **Description:**	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
11863 MITRE NVD	A security feature bypass vulnerability exists in Microsoft Edge when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents. An attacker who exploited the bypass could trick a user into loading a page containing malicious content. To exploit the bypass, an attacker must trick a user into either loading a page containing malicious content or visiting a malicious website. The attacker could also inject the malicious page into either a compromised website or an advertisement network. The security update addresses the bypass by correcting how the Edge CSP validates documents. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11863						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4048956 Security Update	Important	Security Feature Bypass	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4048956 Security Update	Important	Security Feature Bypass	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for	4048952 Security Update	Important	Security Feature Bypass	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11863						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Security Feature Bypass	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4048953 Security Update	Low	Security Feature Bypass	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Security Feature Bypass	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for	4048953 Security Update	Important	Security Feature Bypass	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11863						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Security Feature Bypass	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Security Feature Bypass	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Security Feature Bypass	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11863						
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Security Feature Bypass	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Low	Security Feature Bypass	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11866 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11866 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11866						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows	4048956 Security	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11866						
10 for 32-bit Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 for x64-based Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11866						
Microsoft Edge on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11866						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11866						
Microsoft Edge on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11869 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
11869 MITRE NVD	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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11869						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server	4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11869						
2008 for 32-bit Systems Service Pack 2						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Critical	Remote Code Execution	4041681	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11869						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Critical	Remote Code Execution	4041681	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4047206 IE Cumulative 4048957 Monthly Rollup	Moderate	Remote Code Execution	4041681	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4047206 IE Cumulative	Critical	Remote Code	4041693	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2017-11869						
Windows 8.1 for 32-bit systems	4048958 Monthly Rollup		Execution		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	
Internet Explorer 11 on Windows 8.1 for x64-based systems	4047206 IE Cumulative 4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4047206 IE Cumulative 4048958 Monthly Rollup	Moderate	Remote Code Execution	4041693	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4048958 Monthly Rollup	Critical	Remote Code Execution	4041693	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11869						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4048956 Security Update	Critical	Remote Code Execution	4042895	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11	4048952 Security	Critical	Remote Code	4041689	Base: 7.5 Temporal: 6.7	Yes

CVE-2017-11869						
on Windows 10 Version 1511 for 32-bit Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4048953 Security	Critical	Remote Code	4041691	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2017-11869						
Windows 10 Version 1607 for x64-based Systems	Update		Execution		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	
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11	4048955 Security	Critical	Remote Code	4042198	Base: 7.5 Temporal: 6.7	Yes

CVE-2017-11869						
on Windows 10 Version 1709 for 32-bit Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server, version 1709 (Server Core	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11869						
Installation)						
Internet Explorer 10 on Windows Server 2012	4048959 Monthly Rollup 4047206 IE Cumulative	Moderate	Remote Code Execution	4040685	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-11870 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11870 MITRE NVD	**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	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11870						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11870						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11870						
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11871 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11871 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11871						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11871						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11871						
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11872 - Microsoft Edge Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11872 MITRE NVD	**CVE Title:** Microsoft Edge Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Microsoft Edge improperly handles redirect requests. The vulnerability allows Microsoft Edge to bypass Cross-Origin Resource Sharing (CORS) redirect restrictions, and to follow redirect requests that should otherwise be ignored. An attacker who successfully exploited the vulnerability could force the browser to send data that would otherwise be restricted to a destination website of the attacker's choice. 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,	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 affected Microsoft Edge handles redirect requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11872						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows Server 2016	4048953 Security Update	Low	Security Feature Bypass	4041691	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Important	Security Feature Bypass	4041691	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Security Feature Bypass	4041691	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11872						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Security Feature Bypass	4041676	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Security Feature Bypass	4041676	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11873 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11873 MITRE NVD	**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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11873						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows	4048952 Security	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8	Yes

CVE-2017-11873						
10 Version 1511 for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Critical	Remote Code Execution	4041689	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4048953 Security Update	Moderate	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11873						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Critical	Remote Code Execution	4041691	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Critical	Remote Code Execution	4041676	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11873						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Moderate	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11873						
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4042198	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11874 - Microsoft Edge Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11874 MITRE NVD	**CVE Title:** Microsoft Edge Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Microsoft Edge as a result of how memory is accessed in code compiled by the Edge Just-In-Time (JIT) compiler that allows Control Flow Guard (CFG) to be bypassed. By itself, this CFG bypass vulnerability does not allow arbitrary code execution. However, an attacker could use the CFG bypass vulnerability in conjunction with another vulnerability, such as a remote code execution vulnerability, to run arbitrary code on a target system. To exploit the CFG bypass vulnerability, a user must be logged on and running an affected version of Microsoft Edge. The user would then need to browse to a malicious website.	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the CFG bypass vulnerability by helping to ensure that Microsoft Edge properly handles accessing memory in code compiled by the Edge JIT compiler. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11874						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11874						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Security Feature Bypass	4041676	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4048954 Security Update	Important	Security Feature Bypass	4041676	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Security Feature Bypass	4042198	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4048955 Security Update	Important	Security Feature Bypass	4042198	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11874						
1709 for 64-based Systems						
Microsoft Edge on Windows Server, version 1709 (Server Core Installation)	4048955 Security Update	Low	Security Feature Bypass	4042198	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Only	Important	Security Feature Bypass	4042198	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11876 - Microsoft Project Server Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11876 MITRE NVD	**CVE Title:** Microsoft Project Server Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Project when Microsoft Project Server does not properly manage user sessions. For this Cross-site Request Forgery(CSRF/XSRF) vulnerability to be exploited, the victim must be authenticated to (logged on) the target site. 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 webpage that is designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or Instant Messenger message. An attacker who successfully exploited this vulnerability could read content that the attacker is not authorized to read, use the victim's identity to take actions on the web application on behalf of the victim, such as change permissions and delete content, and inject malicious content in the browser of the victim.	Moderate	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by modifying how Microsoft Project Server manages user session authentication. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11876						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11876						
Microsoft Project Server 2013 Service Pack 1	4011257 Security Update	Moderate	Elevation of Privilege	3203399	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4011244 Security Update	Moderate	Elevation of Privilege	4011217	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11877 - Microsoft Excel Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11877 MITRE NVD	**CVE Title:** Microsoft Excel Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Microsoft Office software by not enforcing macro settings on an Excel document. The security feature bypass by itself does not allow arbitrary code execution. To successfully exploit the vulnerability, an attacker would have to embed a control in an Excel worksheet that specifies a macro should be run. Â To exploit the vulnerability, an attacker would have to convince a user	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	to open a specially crafted file with an affected version of Microsoft Office software. Â The security update addresses the vulnerability by enforcing macro settings on Excel documents. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11877						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11877						
Microsoft Excel 2007 Service Pack 3	4011199 Security Update	Important	Security Feature Bypass	4011062	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel Viewer 2007 Service Pack 3	4011206 Security Update	Important	Security Feature Bypass	4011065	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4011197 Security Update	Important	Security Feature Bypass	4011061	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4011197 Security Update	Important	Security Feature Bypass	4011061	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4011233 Security Update	Important	Security Feature Bypass	4011108	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4011233 Security Update	Important	Security Feature Bypass	4011108	Base: N/A Temporal:	Maybe

CVE-2017-11877						
					N/A Vector: N/A	
Microsoft Excel 2013 RT Service Pack 1	4011233 Security Update	Important	Security Feature Bypass	4011108	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 for Mac	Release Notes Security Update	Important	Security Feature Bypass	4011108	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Excel 2016 (32-bit edition)	4011220 Security Update	Important	Security Feature Bypass	4011050	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	4011220 Security Update	Important	Security Feature Bypass	4011050	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Compatibility Pack Service Pack 3	4011205 Security Update	Important	Security Feature Bypass	4011064	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11878 - Microsoft Excel Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11878 MITRE NVD	**CVE Title:** Microsoft Excel Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office. 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) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11878						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Excel 2007 Service Pack 3	4011199 Security Update	Important	Remote Code Execution	4011062	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel Viewer 2007 Service Pack 3	4011206 Security Update	Important	Remote Code Execution	4011065	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4011197 Security Update	Important	Remote Code Execution	4011061	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4011197 Security Update	Important	Remote Code Execution	4011061	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4011233 Security Update	Important	Remote Code Execution	4011108	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11878						
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4011233 Security Update	Important	Remote Code Execution	4011108	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 RT Service Pack 1	4011233 Security Update	Important	Remote Code Execution	4011108	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (32-bit edition)	4011220 Security Update	Important	Remote Code Execution	4011050	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	4011220 Security Update	Important	Remote Code Execution	4011050	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Compatibility Pack Service Pack 3	4011205 Security Update	Important	Remote Code Execution	4011064	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11879 - ASP.NET Core Elevation Of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11879 MITRE NVD	**CVE Title:** ASP.NET Core Elevation Of Privilege Vulnerability **Description:** An open redirect vulnerability exists in ASP.NET Core that could lead to elevation of privilege. To exploit the vulnerability, an attacker could send a link that has a specially crafted URL, and convince the user to click the link. When an authenticated user clicks the link, the authenticated user's browser session could be redirected to a malicious site that is designed to steal log-in session information such as cookies or authentication tokens. The update addresses the vulnerability by correcting how ASP.NET Core handles open redirect requests. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11879						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
ASP.NET Core 2.0	Commit Security Update	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-11880 - Windows Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11880 MITRE NVD	**CVE Title:** Windows Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. The update addresses the vulnerability by correcting how the Windows kernel initializes objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11880						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11880						
Windows 7 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for	4048957 Monthly	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11880						
Itanium-Based Systems Service Pack 1	Rollup 4048960 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4048957 Monthly Rollup 4048960 Security Only	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server	4049164 Security Update	Important	Information Disclosure	4041681	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11880						
Core installation)						
Windows Server 2012	4048959 Monthly Rollup 4048962 Security Only	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4048959 Monthly Rollup 4048962 Security Only	Important	Information Disclosure	4041690	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11880						
Windows 8.1 for 32-bit systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4048958 Monthly Rollup 404896	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11880						
	1 Security Only					
Windows RT 8.1	4048958 Monthly Rollup	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4048958 Monthly Rollup 4048961 Security Only	Important	Information Disclosure	4041693	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11880						
Windows 10 for x64-based Systems	4048956 Security Update	Important	Information Disclosure	4042895	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4048952 Security Update	Important	Information Disclosure	4041689	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for	4048953 Security	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11880						
32-bit Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4048953 Security Update	Important	Information Disclosure	4041691	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4048954 Security Update	Important	Information Disclosure	4041676	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4048954 Security	Important	Information Disclosure	4041676	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11880						
x64-based Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 64-based Systems	4048955 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4049164 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for	4049164 Security	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2017-11880						
32-bit Systems Service Pack 2	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2	4049164 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4049164 Security Update	Important	Information Disclosure	4042198	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-11882 - Microsoft Office Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11882 MITRE NVD	**CVE Title:** Microsoft Office Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office or Microsoft WordPad 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) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how the affected Office component handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11882						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2007 Service Pack 3	4011276 Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	2553204 Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	2553204 Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	3162047 Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (64-bit editions)	3162047 Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11882						
Microsoft Office 2016 (32-bit edition)	4011262 Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	4011262 Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-11883 - ASP.NET Core Denial Of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11883 MITRE NVD	**CVE Title:** ASP.NET Core Denial Of Service Vulnerability **Description:** A denial of service vulnerability exists when ASP.NET Core improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against a ASP.NET Core web application. The vulnerability can be exploited remotely, without authentication.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the .NET Core application. The update addresses the vulnerability by correcting how the ASP.NET Core web application handles web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11883						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
ASP.NET Core 2.0	Commit Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Yes
ASP.NET Core 1.1	Commit Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Yes
ASP.NET Core 1.0	Commit Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2017-11884 - Microsoft Office Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-11884 MITRE NVD	**CVE Title:** Microsoft Office Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office. 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) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles objects in memory. **FAQ:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	This security update is for the Click-to-Run (C2R) version only. For more information and the current Click-to-Run version number, see Office 365 client update channel releases. **I am being offered this update for software that is not specifically indicated as being affected in the Affected Products 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 Products 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 Products table. Furthermore, when an update applies to Microsoft Office 2010 products, only Microsoft Office 2010 may be specifically listed in the AffectedÂ Products 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 AffectedÂ Products table.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	For more information on this behavior and recommended actions, see Microsoft Knowledge Base Article 830335. For a list of Microsoft Office products that an update may apply to, refer to the Microsoft Knowledge Base Article associated with the specific update. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-11884						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-11884						
Microsoft Excel 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8700 - ASP.NET Core Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8700 MITRE NVD	**CVE Title:** ASP.NET Core Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in ASP.NET Core that allows bypassing Cross-origin Resource Sharing (CORS) configurations. An attacker who successfully exploited the vulnerability could retrieve content, that is normally restricted, from a web application.	Moderate	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by enforcing CORS configuration to prevent its bypass. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/14/2017 08:00:00 Information published.		

Affected Software

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

CVE-2017-8700						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2017-8700						
ASP.NET Core 1.1	Commit Security Update	Moderate	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Maybe
ASP.NET Core 1.0	Commit Security Update	Moderate	Information Disclosure		Base: N/A Temporal: N/A Vector: N/A	Maybe

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