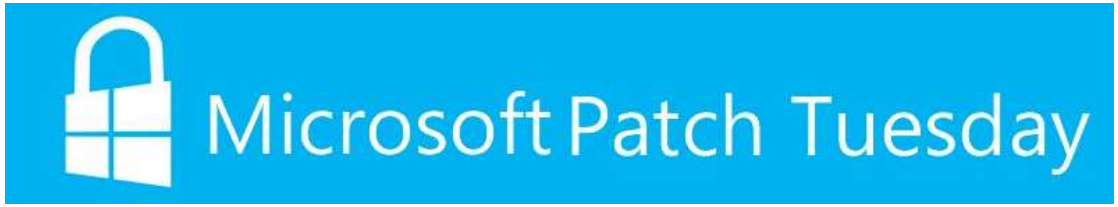
Microsoft's Security Bulletin for March Patches That Fix 68 Security Vulnerabilities

Threat Alert



Date of Release: March 13, 2019

Overview

Microsoft released the March 2019 security patch on Tuesday that fixes 68 vulnerabilities ranging from simple spoofing attacks to remote code execution in various products, including Active Directory, Adobe Flash Player, Azure, Internet Explorer, Microsoft Browsers, Microsoft Edge, Microsoft Graphics Component, Microsoft JET Database Engine, Microsoft Office, Microsoft Office SharePoint, Microsoft Scripting Engine, Microsoft Windows, Microsoft XML, NuGet, Servicing Stack Updates, Skype for Business, Team Foundation Server, Visual Studio, Windows DHCP Client, Windows Hyper-V, Windows Kernel, Windows Kernel-Mode Drivers, Windows Print Spooler Components, Windows SMB Server, and Windows Subsystem for Linux.

Details can be found in the following table.

Product	CVE ID	CVE Title	Severity Level

Active Directory	CVE-2019-0683	Active Directory Privilege Escalation Vulnerability	Important
Adobe Flash Player	ADV190008	March 2019 Adobe Flash Security Update	Low
Azure	CVE-2019-0816	Azure SSH Keypairs Security Feature Bypass Vulnerability	Moderate
Internet Explorer	CVE-2019-0761	Internet Explorer Security Feature Bypass Vulnerability	Low
Internet Explorer	CVE-2019-0763	Internet Explorer Memory Corruption Vulnerability	Moderate
Internet Explorer	CVE-2019-0768	Internet Explorer Security Feature Bypass Vulnerability	Important
Microsoft Browsers	CVE-2019-0762	Microsoft Browsers Security Feature Bypass Vulnerability	Low

Microsoft Browsers	CVE-2019-0780	Microsoft Browser Memory Corruption Vulnerability	Important
Microsoft Edge	CVE-2019-0612	Microsoft Edge Security Feature Bypass Vulnerability	Important
Microsoft Edge	CVE-2019-0678	Microsoft Edge Privilege Escalation Vulnerability	Important
Microsoft Edge	CVE-2019-0779	Microsoft Edge Memory Corruption Vulnerability	Important
Microsoft Graphics Component	CVE-2019-0774	Windows GDI Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2019-0797	Win32k Privilege Escalation Vulnerability	Important
Microsoft Graphics Component	CVE-2019-0808	Win32k Privilege Escalation Vulnerability	Important

Microsoft Graphics Component	CVE-2019-0614	Windows GDI Information Disclosure Vulnerability	Important
Microsoft JET Database Engine	CVE-2019-0617	Jet Database Engine Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2019-0748	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability	Important
Microsoft Office SharePoint	CVE-2019-0778	Microsoft Office SharePoint XSS Vulnerability	Important
Microsoft Scripting Engine	CVE-2019-0609	Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0611	Chakra Scripting Engine Memory Corruption Vulnerability	Low
Microsoft Scripting Engine	CVE-2019-0639	Scripting Engine Memory Corruption Vulnerability	Moderate

Microsoft Scripting Engine	CVE-2019-0746	Chakra Scripting Engine Memory Corruption Vulnerability	Important
Microsoft Scripting Engine	CVE-2019-0769	Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0770	Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0771	Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0772	Windows VBScript Engine Remote Code Execution Vulnerability	Important
Microsoft Scripting Engine	CVE-2019-0773	Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0783	Scripting Engine Memory Corruption Vulnerability	Important
Microsoft Scripting Engine	CVE-2019-0592	Chakra Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0665	Windows VBScript Engine Remote Code Execution Vulnerability	Important

Microsoft Scripting Engine	CVE-2019-0666	Windows VBScript Engine Remote Code Execution Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0667	Windows VBScript Engine Remote Code Execution Vulnerability	Critical
Microsoft Scripting Engine	CVE-2019-0680	Scripting Engine Memory Corruption Vulnerability	Critical
Microsoft Windows	CVE-2019-0754	Windows Denial-of-Service Vulnerability	Important
Microsoft Windows	CVE-2019-0765	Comctl32 Remote Code Execution Vulnerability	Important
Microsoft Windows	CVE-2019-0766	Microsoft Windows Privilege Escalation Vulnerability	Important
Microsoft Windows	CVE-2019-0784	Windows ActiveX Remote Code Execution Vulnerability	Critical

Microsoft Windows	ADV190009	SHA-2 Code Sign Support Advisory	Unknown
Microsoft Windows	ADV190010	Best Practices Regarding Sharing of a Single User Account Across Multiple Users	Unknown
Microsoft Windows	CVE-2019-0603	Windows Deployment Services TFTP Server Remote Code Execution Vulnerability	Critical
Microsoft XML	CVE-2019-0756	MS XML Remote Code Execution Vulnerability	Critical
NuGet	CVE-2019-0757	NuGet Package Manager Tampering Vulnerability	Important
Servicing Stack Updates	ADV990001	Latest Servicing Stack Updates	Critical
Skype for Business	CVE-2019-0798	Skype for Business and Lync Spoofing Vulnerability	Important

Team Foundation Server	CVE-2019-0777	Team Foundation Server Cross-site Scripting Vulnerability	Low
Visual Studio	CVE-2019-0809	Visual Studio Remote Code Execution Vulnerability	Important
Windows DHCP Client	CVE-2019-0697	Windows DHCP Client Remote Code Execution Vulnerability	Critical
Windows DHCP Client	CVE-2019-0698	Windows DHCP Client Remote Code Execution Vulnerability	Critical
Windows DHCP Client	CVE-2019-0726	Windows DHCP Client Remote Code Execution Vulnerability	Critical
Windows Hyper-V	CVE-2019-0690	Windows Hyper-V Denial-of-Service Vulnerability	Important
Windows Hyper-V	CVE-2019-0695	Windows Hyper-V Denial-of-Service Vulnerability	Important
Windows Hyper-V	CVE-2019-0701	Windows Hyper-V Denial-of-Service Vulnerability	Important
Windows Kernel	CVE-2019-0755	Windows Kernel Information Disclosure Vulnerability	Important

Windows Kernel	CVE-2019-0767	Windows Kernel Information Disclosure Vulnerability	Important
Windows Kernel	CVE-2019-0775	Windows Kernel Information Disclosure Vulnerability	Important
Windows Kernel	CVE-2019-0782	Windows Kernel Information Disclosure Vulnerability	Important
Windows Kernel	CVE-2019-0696	Windows Kernel Information Disclosure Vulnerability	Important
Windows Kernel	CVE-2019-0702	Windows Kernel Information Disclosure Vulnerability	Important
Windows Kernel-Mode Drivers	CVE-2019-0776	Win32k Information Disclosure Vulnerability	Important
Windows Print Spooler Components	CVE-2019-0759	Windows Print Spooler Information Disclosure Vulnerability	Important
Windows SMB Server	CVE-2019-0703	Windows SMB Information Disclosure Vulnerability	Important
Windows SMB Server	CVE-2019-0704	Windows SMB Information Disclosure Vulnerability	Important

Windows SMB Server	CVE-2019-0821	Windows SMB Information Disclosure Vulnerability	Important
Windows Subsystem for Linux	CVE-2019-0682	Windows Subsystem for Linux Privilege Escalation Vulnerability	Important
Windows Subsystem for Linux	CVE-2019-0689	Windows Subsystem for Linux Privilege Escalation Vulnerability	Important
Windows Subsystem for Linux	CVE-2019-0692	Windows Subsystem for Linux Privilege Escalation Vulnerability	Important
Windows Subsystem for Linux	CVE-2019-0693	Windows Subsystem for Linux Privilege Escalation Vulnerability	Important
Windows Subsystem for Linux	CVE-2019-0694	Windows Subsystem for Linux Privilege Escalation Vulnerability	Important

Recommended Mitigation Measures

Microsoft has released the January 2019 security patch to fix these issues. Please install the patch as soon as possible.

Appendix

ADV190008 - March 2019 Adobe Flash Security Update

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190008 MITRE NVD	**CVE Title:** March 2019 Adobe Flash Security Update **Description:** This security update addresses minor security fixes, which are described in Adobe Security Bulletin APSB19-12. **FAQ:** **How could an attacker exploit these vulnerabilities?** In a web-based attack scenario where the user is using Internet Explorer for the desktop, an attacker could host a specially crafted website that is designed to exploit any of these vulnerabilities through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit any of these vulnerabilities. In all cases,	Low	Defense in Depth

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by clicking a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email. In a web-based attack scenario where the user is using Internet Explorer in the Windows 8-style UI, an attacker would first need to compromise a website already listed in the Compatibility View (CV) list. An attacker could then host a website that contains specially crafted Flash content designed to exploit any of these vulnerabilities through Internet Explorer and then convince a user to view the website. An attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by clicking a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by opening an attachment sent through email. For more information about Internet Explorer and the CV List, please see the MSDN Article, Developer Guidance for websites with content for Adobe Flash Player in Windows 8. **Mitigations:** **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workaround refers to a setting or configuration change that would help block known attack vectors before you apply the update. **Prevent Adobe Flash Player from running** You can disable attempts to instantiate Adobe Flash Player in Internet Explorer and other applications that honor the kill bit feature, such as Office 2007 and Office 2010, by setting the kill bit for the control in the registry. **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. To set the kill bit for the control in the registry, perform the following steps: 1. Paste the following into a text file and save it with the .reg file extension. 2. Windows Registry Editor Version 5.00 3. [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] 4. "Compatibility Flags"=dword:00000400 5. 6. [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] 7. "Compatibility Flags"=dword:00000400		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	8. Double-click the .reg file to apply it to an individual system. You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, Group Policy collection. **Note** You must restart Internet Explorer for your changes to take effect. **Impact of workaround**. There is no impact as long as the object is not intended to be used in Internet Explorer. **How to undo the workaround.** Delete the registry keys that were added in implementing this workaround. **Prevent Adobe Flash Player from running in Internet Explorer through Group Policy Note** The Group Policy MMC snap-in can be used to set policy for a machine, for an organizational unit, or for an entire domain. For more information about Group Policy, visit the following Microsoft Web sites: Group Policy Overview 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. 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**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	3. Double-click **Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects**. 4. Change the setting to Enabled. 5. Click **Apply** and then click **OK** to return to the Group Policy Management Console. 6. Refresh Group Policy on all systems or wait for the next scheduled Group Policy refresh interval for the settings to take effect. **Prevent Adobe Flash Player from running in Office 2010 on affected systems Note** This workaround does not prevent Adobe Flash Player from running in Internet Explorer. **Warning** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk. For detailed steps that you can use to prevent a control from running in Internet Explorer, see Microsoft Knowledge Base Article 240797. Follow the steps in the article to create a Compatibility Flags value in the registry to prevent a COM object from being instantiated in Internet Explorer. To disable Adobe Flash Player in Office 2010 only, set the kill bit for the ActiveX control for Adobe Flash Player in the registry using the following steps: 1. Create a text file named Disable_Flash.reg with the following contents:		

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. 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**.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To re-enable ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, perform the following steps: 1. Click File, click Options, click Trust Center, and then click Trust Center Settings. 2. Click ActiveX Settings in the left-hand pane, and then deselect Disable all controls without notifications. 3. Click OK to save your settings. **Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones** You can help protect against exploitation of these vulnerabilities by changing your settings for the Internet security zone to block ActiveX controls and Active Scripting. You can do this by setting your browser security to High. To raise the browsing security level in Internet Explorer, perform the following steps: 1. On the Internet Explorer **Tools** menu, click** Internet Option**s. 2. In the **Internet Options** dialog box, click the **Security** tab, and then click **Internet**. 3. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 4. Click **Local intranet**. 5. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	6. Click **OK** to accept the changes and return to Internet Explorer. **Note** If no slider is visible, click **Default Level**, and then move the slider to **High**. **Note** Setting the level to High may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly even with the security setting set to High. **Impact of workaround**. There are side effects to blocking ActiveX Controls and Active Scripting. Many websites on the Internet or an intranet use ActiveX or Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX Controls to provide menus, ordering forms, or even account statements. Blocking ActiveX Controls or Active Scripting is a global setting that affects all Internet and intranet sites. If you do not want to block ActiveX Controls or Active Scripting for such sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". **Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone** You can help protect against exploitation of these vulnerabilities by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone. To do this, perform the following steps: 1. In Internet Explorer, click **Internet Options** on the **Tools** menu. 2. Click the **Security** tab.		

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	zone and in the Local intranet zone, you can add sites that you trust to the Internet Explorer Trusted sites zone. This will allow you to continue to use trusted websites exactly as you do today, while helping to protect you from this attack on untrusted sites. We recommend that you add only sites that you trust to the Trusted sites zone. To do this, perform the following steps: 1. In Internet Explorer, click **Tools**, click **Internet Options**, and then click the **Security** tab. 2. In the **Select a web content zone to specify its current security settings** box, click **Trusted Sites**, and then click **Sites**. 3. If you want to add sites that do not require an encrypted channel, click to clear the **Require server verification (https:) for all sites in this zone** check box. 4. In the **Add this website to the zone** box, type the URL of a site that you trust, and then click **Add**. 5. Repeat these steps for each site that you want to add to the zone. 6. Click **OK** two times to accept the changes and return to Internet Explorer. **Note** Add any sites that you trust not to take malicious action on your system. Two sites in particular that you may want to add are ***.windowsupdate.microsoft.com** and ***.update.microsoft.com**. These are the sites that will host the update, and they require an ActiveX control to install the update.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

ADV190008						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Adobe Flash Player on Windows Server 2012	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190008						
Adobe Flash Player on Windows 8.1 for 32-bit systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for x64-based systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2012 R2	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows RT 8.1	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 for 32-bit Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 for x64-based Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal:	Yes

ADV190008						
					N/A Vector: N/A	
Adobe Flash Player on Windows Server 2016	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190008						
Adobe Flash Player on Windows 10 Version 1709 for 32-bit Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for x64-based Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1803 for 32-bit Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1803 for x64-based Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1803 for ARM64-based Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1809 for 32-bit Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal:	Yes

ADV190008						
					N/A Vector: N/A	
Adobe Flash Player on Windows 10 Version 1809 for x64-based Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1809 for ARM64-based Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2019	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for ARM64-based Systems	4489907 Security Update	Low	Defense in Depth	4480979	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190009 - SHA-2 Code Sign Support Advisory

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190009 MITRE NVD	**CVE Title:** SHA-2 Code Sign Support Advisory **Description:** Microsoft is announcing the release of SHA-2 code sign support for Windows 7 SP1, and Windows Server 2008 R2 SP1. Please see 2019 SHA-2 Code Signing Support requirement for Windows and WSUS for more information. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.	Unknown	Defense in Depth

Affected Software

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

ADV190009						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4474419 Security Update		Defense in Depth	3212642	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 7 for x64-based Systems Service Pack 1	4474419 Security Update		Defense in Depth	3212642	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4474419 Security Update		Defense in Depth	3212642	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4474419 Security Update		Defense in Depth	3212642	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190009						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4474419 Security Update		Defense in Depth	3212642	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV190010 - Best Practices Regarding Sharing of a Single User Account Across Multiple Users

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV190010 MITRE NVD	**CVE Title:** Best Practices Regarding Sharing of a Single User Account Across Multiple Users **Description:** Microsoft strongly recommends customers avoid the use of a 'common' or 'shared' Windows logon account. A single user account should never be shared amongst different users. This is especially true when users are logging into the same physical machine. Customers who have solutions designed this way are encouraged to engage their solution vendors for assistance in configuring their product to support independent user accounts.	Unknown	Unknown

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Microsoft considers the practice of sharing the same user account with multiple users a significant security risk. There is no security boundary between sessions using the same user account on the same Windows client or server. For more information on User and Session boundaries, please see the Security Servicing Criteria for Windows. # FAQ **What is a session?** A session consists of all the processes and other system objects which represent a single user's logon session.â€¯ These objects include all windows, desktops and windows stations. **How can Windows be configured to allow a single user to have multiple sessions?** This can be achieved by either First-party or Third-party applications. One example, applicable to some versions of Windows Server, is by enabling the group policy setting under: Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The setting is "Restrict Remote Desktop Services users to a single Remote Desktop Services session". If this policy is disabled, then users are allowed to make multiple simultaneous remote connections using the same user account to an RDS server via Remote Desktop Services. **Is this information related to a security vulnerability?** No, this is guidance on best practices in your network environment. There are no security updates planned for this issue. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

ADV190010						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
None Available					Base: N/A Temporal: N/A Vector: N/A	

ADV990001 - Latest Servicing Stack Updates

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV990001 MITRE NVD	**CVE Title:** Latest Servicing Stack Updates **Description:** This is a list of the latest servicing stack updates for each operating sytem. This list will be updated whenever a new servicing stack update is released. It is important to install the latest servicing stack update.	Critical	Defense in Depth

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **1. Why are all of the Servicing Stack Updates (SSU) critical updates?** The SSUs are classified as Critical updates. This does not indicate that there is a critical vulnerability being addressed in the update. **2. When was the most recent SSU released for each version of Microsoft Windows?** Please refer to the following table for the most recent SSU release. We will update the entries any time a new SSU is released:		

Product	SSU Package	Date Released
Windows Server 2008	955430	May 2009
Windows 7/Server 2008 R2	4490628	March 2019
Windows Server 2012	3173426	July 2016
Windows 8.1/Server 2012 R2	3173424	July 2016
Windows 10	4093430	April 2018
Windows 10 Version 1607/Server 2016	4485447	February 2019
Windows 10 Version 1703	4487327	February 2019
Windows 10 1709/Windows Server, version 1709	4485448	February 2019
Windows 10 1803/Windows Server, version 1803	4485449	February 2019

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Windows 10 1809/Server 2019 4470788 December 2018 **Mitigations:** None **Workarounds:** None **Revision:** 1.0 11/13/2018 08:00:00 Information published. 5.1 02/13/2019 08:00:00 In the Security Updates table, corrected the Servicing Stack Update (SSU) for Windows 10 Version 1809 for x64-based Systems to 4470788. This is an informational change only. 3.2 12/12/2018 08:00:00 Fixed a typo in the FAQ. 2.0 12/05/2018 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1809 and Windows Server 2019. See the FAQ section for more information. 3.1 12/11/2018 08:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Updated supersedence information. This is an informational change only. 2.0 12/05/2018 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1809 and Windows Server 2019. See the FAQ section for more information. 1.1 11/14/2018 08:00:00 Corrected the link to the Windows Server 2008 Servicing Stack Update. This is an informational change only. 5.0 02/12/2019 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1607, Windows Server 2016, and Windows Server 2016 (Server Core installation); Windows 10 Version 1703; Windows 10 Version 1709 and Windows Server, version 1709 (Server Core Installation); Windows 10 Version 1803, and Windows Server, version 1803 (Server Core Installation). See the FAQ section for more information. 1.2 12/03/2018 08:00:00 FAQs have been added to further explain Security Stack Updates. The FAQs include a table that indicates the most recent SSU release for each Windows version. This is an informational change only. 6.0 03/12/2019 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	A Servicing Stack Update has been released for Windows 7 and Windows Server 2008 R2 and Windows Server 2008 R2 (Server Core installation). See the FAQ section for more information. 5.2 02/14/2019 08:00:00 In the Security Updates table, corrected the Servicing Stack Update (SSU) for Windows 10 Version 1803 for x64-based Systems to 4485449. This is an informational change only. 3.0 12/11/2018 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1709, Windows Server, version 1709 (Server Core Installation), Windows 10 Version 1803, and Windows Server, version 1803 (Server Core Installation). See the FAQ section for more information. 4.0 01/08/2019 08:00:00 A Servicing Stack Update has been released for Windows 10 Version 1703. See the FAQ section for more information.		

Affected Software

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

ADV990001						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4490628 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 7 for x64-based Systems Service Pack 1	4490628 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4490628 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4490628 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4490628 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	955430 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012	3173426 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 (Server Core installation)	3173426 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for 32-bit systems	3173424 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 8.1 for x64-based systems	3173424 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2012 R2	3173424 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows Server 2012 R2 (Server Core installation)	3173424 Servicing Stack Update	Critical	Defense in Depth		Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for 32-bit Systems	4093430 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 for x64-based Systems	4093430 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016	4485447 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1607 for 32-bit Systems	4485447 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows 10 Version 1607 for x64-based Systems	4485447 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2016 (Server Core installation)	4485447 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for 32-bit Systems	4487327 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1703 for x64-based Systems	4487327 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for 32-bit Systems	4485448 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for x64-based Systems	4485448 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows Server, version 1709 (Server Core Installation)	4485448 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for 32-bit Systems	4485449 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for x64-based Systems	4485449 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server, version 1803 (Server Core Installation)	4485449 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1803 for ARM64-based Systems	4485449 Servicing Stack Update	Critical	Defense in Depth	4021701	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV990001						
Windows 10 Version 1809 for 32-bit Systems	4470788 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for x64-based Systems	4470788 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1809 for ARM64-based Systems	4470788 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019	4470788 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2019 (Server Core installation)	4470788 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows 10 Version 1709 for ARM64-based Systems	4485448 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal:	Yes

ADV990001						
					N/A Vector: N/A	
Windows Server 2008 for Itanium-Based Systems Service Pack 2	955430 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	955430 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	955430 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	955430 Servicing Stack Update	Critical	Defense in Depth	4465664	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0592 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0592 MITRE NVD	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.	Critical	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0592						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0592						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Critical	Elevation of Privilege	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for x64-based Systems	4489899 Security Update	Critical	Elevation of Privilege	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for ARM64-based Systems	4489899 Security Update	Critical	Elevation of Privilege	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 2019	4489899 Security Update	Moderate	Elevation of Privilege	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0592						
ChakraCore	Release Notes Security Update	Critical	Elevation of Privilege	4487044	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0603 - Windows Deployment Services TFTP Server Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0603 MITRE NVD	**CVE Title:** Windows Deployment Services TFTP Server Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that Windows Deployment Services TFTP Server handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code with elevated permissions on a target system.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker could create a specially crafted request, causing Windows to execute arbitrary code with elevated permissions. The security update addresses the vulnerability by correcting how Windows Deployment Services TFTP Server handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0603						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Critical	Remote Code Execution	4486563	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4489878 Monthly Rollup 4489885 Security Only	Critical	Remote Code Execution	4486563	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4489878 Monthly Rollup 4489885 Security Only	Critical	Remote Code Execution	4486563	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0603						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Critical	Remote Code Execution	4486563	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4489878 Monthly Rollup 4489885 Security Only	Critical	Remote Code Execution	4486563	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4489880 Monthly Rollup 4489876 Security	Critical	Remote Code Execution	4487019	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0603						
Core installation)	Only					
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Critical	Remote Code Execution	4487025	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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)	4489884 Security Only 4489891 Monthly Rollup	Critical	Remote Code Execution	4487025	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4489881 Monthly Rollup 4489883 Security Only	Critical	Remote Code Execution	4487000	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2019-0603						
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security Only	Critical	Remote Code Execution	4487000	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Critical	Remote Code Execution	4487000	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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)	4489881 Monthly Rollup 4489883 Security	Critical	Remote Code Execution	4487000	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2019-0603						
	Only					
Windows Server 2016	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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)	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0603						
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0603						
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4489880 Monthly Rollup 4489876 Security Only	Critical	Remote Code Execution	4487019	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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	4489880 Monthly Rollup	Critical	Remote Code Execution	4487019	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0603						
Systems Service Pack 2	4489876 Security Only				Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Critical	Remote Code Execution	4487019	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/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)	4489880 Monthly Rollup 4489876 Security Only	Critical	Remote Code Execution	4487019	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0609 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0609 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 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0609						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Critical	Remote Code Execution	4486474	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	4489878 Monthly Rollup 4489873 IE Cumulative	Critical	Remote Code Execution	4486474	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	4489878 Monthly Rollup 4489873	Moderate	Remote Code Execution	4486474	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-2019-0609						
Server 2008 R2 for x64-based Systems Service Pack 1	IE Cumulative					
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4489873 IE Cumulative 4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	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	4489873 IE Cumulative 4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	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	4489873 IE Cumulative	Moderate	Remote Code Execution	4487000	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-0609						
Windows Server 2012 R2	4489881 Monthly Rollup				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	
Internet Explorer 11 on Windows RT 8.1	4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	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	4489872 Security Update	Critical	Remote Code Execution	4487018	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	4489872 Security Update	Critical	Remote Code Execution	4487018	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-2019-0609						
Internet Explorer 11 on Windows Server 2016	4489882 Security Update	Moderate	Remote Code Execution	4487026	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	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Critical	Remote Code Execution	4487026	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-2019-0609						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Critical	Remote Code Execution	4487020	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	4489871 Security Update	Critical	Remote Code Execution	4487020	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	4489886 Security Update	Critical	Remote Code Execution	4486996	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-2019-0609						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	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 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	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	4489868 Security Update	Critical	Remote Code Execution	4487017	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-2019-0609						
1803 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	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 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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	4489899 Security	Critical	Remote Code Execution	4487044	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0609						
Windows 10 Version 1809 for x64-based Systems	Update				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 1809 for ARM64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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 2019	4489899 Security Update	Moderate	Remote Code Execution	4487044	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	4489886 Security	Critical	Remote Code Execution	4486996	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0609						
Windows 10 Version 1709 for ARM64-based Systems	Update				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	
Microsoft Edge on Windows 10 for 32-bit Systems	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Moderate	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0609						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0609						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0609						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for x64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for ARM64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0609						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for ARM64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0609						
Microsoft Edge on Windows Server 2019	4489899 Security Update	Moderate	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 ARM64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4486996	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0611 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0611 MITRE NVD	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory.	Low	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0611						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0611						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Information Disclosure	4487020	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	4489871 Security Update	Important	Information Disclosure	4487020	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	4489886 Security Update	Important	Information Disclosure	4486996	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	4489886 Security Update	Important	Information Disclosure	4486996	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-2019-0611						
1709 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Information Disclosure	4487017	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 1803 for x64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	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 1803 for ARM64-	4489868 Security Update	Important	Information Disclosure	4487017	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-2019-0611						
based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Information Disclosure	4487044	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 1809 for x64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	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 1809 for ARM64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	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-2019-0611						
Microsoft Edge on Windows Server 2019	4489899 Security Update	Low	Information Disclosure	4487044	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 ARM64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security Update	Important	Information Disclosure	4486996	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0612 - Microsoft Edge Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0612 MITRE NVD	**CVE Title:** Microsoft Edge Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Click2Play protection in Microsoft Edge improperly handles flash objects. By itself, this bypass vulnerability does not allow arbitrary code execution. However, an attacker could use the 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. The security update addresses the bypass vulnerability by helping to ensure that Click2Play protection Microsoft Edge properly handles flash objects. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0612						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Security Feature Bypass	4487020	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0612						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Security Feature Bypass	4487020	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/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	4489886 Security Update	Important	Security Feature Bypass	4486996	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/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 x64-based Systems	4489886 Security Update	Important	Security Feature Bypass	4486996	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/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 1803	4489868 Security Update	Important	Security Feature Bypass	4487017	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0612						
for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Security Feature Bypass	4487017	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/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 1803 for ARM64-based Systems	4489868 Security Update	Important	Security Feature Bypass	4487017	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/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 1809 for 32-bit Systems	4489899 Security Update	Important	Security Feature Bypass	4487044	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0612						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Security Feature Bypass	4487044	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/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 1809 for ARM64-based Systems	4489899 Security Update	Important	Security Feature Bypass	4487044	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4489899 Security Update	Low	Security Feature Bypass	4487044	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/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 ARM64-	4489886 Security Update	Important	Security Feature Bypass	4486996	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0612						
based Systems						

CVE-2019-0614 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0614 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0614						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0614						
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0614						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0614						
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 8.1 for x64-	4489881 Monthly	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2	Unknown

CVE-2019-0614						
based systems	Rollup 4489883 Security Only				Vector: CVSS: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	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0614						
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489872 Security Update	Important	Information Disclosure	4487018	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0614						
(Server Core installation)	Update				Vector: CVSS: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 1703 for 32-bit Systems	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489886 Security	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0614						
1709 (Server Core Installation)	Update				Vector: CVSS: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 1803 for 32-bit Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 for x64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 (Server Core Installation)	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 for ARM64-	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0614						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1809 for x64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1809 for ARM64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 2019	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 2019	4489899 Security	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0614						
(Server Core installation)	Update				Vector: CVSS: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 ARM64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0614						
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0617 - Jet Database Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0617 MITRE NVD	**CVE Title:** Jet Database Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Windows Jet Database Engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

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

CVE-2019-0617						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Remote Code Execution	4486563	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4489878 Monthly Rollup	Important	Remote Code Execution	4486563	Base: 7.8 Temporal: 7	Yes

CVE-2019-0617						
Service Pack 1	4489885 Security Only				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4489878 Monthly Rollup 4489885 Security Only	Important	Remote Code Execution	4486563	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Remote Code Execution	4486563	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0617						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Remote Code Execution	4486563	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Remote Code Execution	4487019	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Important	Remote Code Execution	4487025	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0617						
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Important	Remote Code Execution	4487025	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4489881 Monthly Rollup 4489883 Security Only	Important	Remote Code Execution	4487000	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security Only	Important	Remote Code Execution	4487000	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2019-0617						
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Remote Code Execution	4487000	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Remote Code Execution	4487000	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4489881 Monthly Rollup 4489883 Security Only	Important	Remote Code Execution	4487000	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Remote Code Execution	4487018	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0617						
Windows 10 for x64-based Systems	4489872 Security Update	Important	Remote Code Execution	4487018	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4489882 Security Update	Important	Remote Code Execution	4487026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Important	Remote Code Execution	4487026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Remote Code Execution	4487026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4489882 Security Update	Important	Remote Code Execution	4487026	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703	4489871 Security	Important	Remote Code Execution	4487020	Base: 7.8 Temporal: 7	Yes

CVE-2019-0617						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Remote Code Execution	4487020	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Remote Code Execution	4487017	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0617						
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Important	Remote Code Execution	4487017	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Remote Code Execution	4487044	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0617						
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security Update	Important	Remote Code Execution	4487044	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4489899 Security Update	Important	Remote Code Execution	4487044	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems	4489880 Monthly Rollup 4489876 Security	Important	Remote Code Execution	4487019	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0617						
Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Remote Code Execution	4487019	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Remote Code Execution	4487019	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4489880 Monthly Rollup 4489876 Security Only	Important	Remote Code Execution	4487019	Base: 7.8 Temporal: 7 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0617						
Core installation)						

CVE-2019-0639 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0639 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how the ChakraCore scripting engine handles objects in memory.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0639						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0639						
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for x64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for ARM64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0639						
for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for ARM64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 2019	4489899 Security Update	Moderate	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0639						
	Update					

CVE-2019-0665 - Windows VBScript Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0665 MITRE NVD	**CVE Title:** Windows VBScript Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0665						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Important	Remote Code Execution	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems	4489878 Monthly Rollup 4489873 IE Cumulative	Important	Remote Code Execution	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0665						
Service Pack 1						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Low	Remote Code Execution	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4489873 IE Cumulative 4489881 Monthly Rollup	Important	Remote Code Execution	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on	4489873 IE Cumulative 4489881	Important	Remote Code Execution	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0665						
Windows 8.1 for x64-based systems	Monthly Rollup					
Internet Explorer 11 on Windows Server 2012 R2	4489873 IE Cumulative 4489881 Monthly Rollup	Low	Remote Code Execution	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows RT 8.1	4489881 Monthly Rollup	Important	Remote Code Execution	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4489872 Security Update	Important	Remote Code Execution	4487018	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0665						
Internet Explorer 11 on Windows 10 for x64-based Systems	4489872 Security Update	Important	Remote Code Execution	4487018	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows Server 2016	4489882 Security Update	Low	Remote Code Execution	4487026	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Important	Remote Code Execution	4487026	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0665						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Remote Code Execution	4487026	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Remote Code Execution	4487020	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10	4489871 Security Update	Important	Remote Code Execution	4487020	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0665						
Version 1703 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0665						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Remote Code Execution	4487017	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10	4489868 Security Update	Important	Remote Code Execution	4487017	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0665						
Version 1803 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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 1809 for x64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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-2019-0665						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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 2019	4489899 Security Update	Low	Remote Code Execution	4487044	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	4489886 Security Update	Important	Remote Code Execution	4486996	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0665						
ARM64-based Systems						
Internet Explorer 10 on Windows Server 2012	4489873 IE Cumulative 4489891 Monthly Rollup	Low	Remote Code Execution	4487025	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0666 - Windows VBScript Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0666	**CVE Title:** Windows VBScript Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0666						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for	4489880 Monthly Rollup 4489873 IE Cumulative	Moderate	Remote Code Execution	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0666						
32-bit Systems Service Pack 2						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489873 IE Cumulative	Moderate	Remote Code Execution	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Critical	Remote Code Execution	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0666						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Critical	Remote Code Execution	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Moderate	Remote Code Execution	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on	4489873 IE Cumulative 4489881	Critical	Remote Code Execution	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0666						
Windows 8.1 for 32-bit systems	Monthly Rollup					
Internet Explorer 11 on Windows 8.1 for x64-based systems	4489873 IE Cumulative 4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows Server 2012 R2	4489873 IE Cumulative 4489881 Monthly Rollup	Moderate	Remote Code Execution	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows RT 8.1	4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0666						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows Server 2016	4489882 Security Update	Moderate	Remote Code Execution	4487026	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on	4489882 Security	Critical	Remote Code Execution	4487026	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0666						
Windows 10 Version 1607 for 32-bit Systems	Update					
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0666						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1709 for	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0666						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0666						
1803 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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	4489899 Security	Critical	Remote Code Execution	4487044	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0666						
Windows 10 Version 1809 for ARM64-based Systems	Update				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 2019	4489899 Security Update	Moderate	Remote Code Execution	4487044	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 ARM64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0666						
Internet Explorer 10 on Windows Server 2012	4489873 IE Cumulative 4489891 Monthly Rollup	Moderate	Remote Code Execution	4487025	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0667 - Windows VBScript Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0667 MITRE NVD	**CVE Title:** Windows VBScript Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could	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. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

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

CVE-2019-0667						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems	4489880 Monthly Rollup 4489873 IE Cumulative	Moderate	Remote Code Execution	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0667						
Service Pack 2						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489873 IE Cumulative	Moderate	Remote Code Execution	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Critical	Remote Code Execution	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0667						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Critical	Remote Code Execution	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Moderate	Remote Code Execution	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on	4489873 IE Cumulative 4489881	Critical	Remote Code Execution	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0667						
Windows 8.1 for 32-bit systems	Monthly Rollup					
Internet Explorer 11 on Windows 8.1 for x64-based systems	4489873 IE Cumulative 4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows Server 2012 R2	4489873 IE Cumulative 4489881 Monthly Rollup	Moderate	Remote Code Execution	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows RT 8.1	4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0667						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows Server 2016	4489882 Security Update	Moderate	Remote Code Execution	4487026	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on	4489882 Security	Critical	Remote Code Execution	4487026	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0667						
Windows 10 Version 1607 for 32-bit Systems	Update					
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0667						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1709 for	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0667						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0667						
1803 for ARM64-based Systems						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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	4489899 Security	Critical	Remote Code Execution	4487044	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0667						
Windows 10 Version 1809 for ARM64-based Systems	Update				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 2019	4489899 Security Update	Moderate	Remote Code Execution	4487044	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 ARM64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0667						
Internet Explorer 10 on Windows Server 2012	4489873 IE Cumulative 4489891 Monthly Rollup	Moderate	Remote Code Execution	4487025	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0678 - Microsoft Edge Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0678 MITRE NVD	**CVE Title:** Microsoft Edge Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain. In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force users to view the attacker-	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. An attacker who successfully exploited this vulnerability could elevate privileges in affected versions of Microsoft Edge. The security update addresses the vulnerability by helping to ensure that cross-domain policies are properly enforced in Microsoft Edge. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0678						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows Server 2016	4489882 Security Update	Low	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Important	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Important	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0678						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489871 Security Update	Important	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0678						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for 32-bit Systems	4489868 Security Update	Important	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for x64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489868 Security	Important	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0678						
Version 1803 for ARM64-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 1809 for 32-bit Systems	4489899 Security Update	Important	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for x64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for	4489899 Security Update	Important	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0678						
ARM64-based Systems						
Microsoft Edge on Windows Server 2019	4489899 Security Update	Low	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 ARM64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0680 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0680 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 Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	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 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0680						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Critical	Remote Code Execution	4486474	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	4489878 Monthly Rollup 4489873 IE Cumulative	Critical	Remote Code Execution	4486474	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	4489878 Monthly Rollup	Moderate	Remote Code Execution	4486474	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-0680						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489873 IE Cumulative				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	
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4489873 IE Cumulative 4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	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	4489873 IE Cumulative 4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	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-2019-0680						
Internet Explorer 11 on Windows Server 2012 R2	4489873 IE Cumulative 4489881 Monthly Rollup	Moderate	Remote Code Execution	4487000	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	4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	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	4489872 Security Update	Critical	Remote Code Execution	4487018	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	4489872 Security Update	Critical	Remote Code Execution	4487018	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-2019-0680						
x64-based Systems						
Internet Explorer 11 on Windows Server 2016	4489882 Security Update	Moderate	Remote Code Execution	4487026	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	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4489882 Security Update	Critical	Remote Code Execution	4487026	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-2019-0680						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Critical	Remote Code Execution	4487020	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	4489871 Security Update	Critical	Remote Code Execution	4487020	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	4489886 Security Update	Critical	Remote Code Execution	4486996	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-2019-0680						
1709 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	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 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	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	4489868 Security Update	Critical	Remote Code Execution	4487017	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-2019-0680						
10 Version 1803 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	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 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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-2019-0680						
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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 1809 for ARM64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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 2019	4489899 Security Update	Moderate	Remote Code Execution	4487044	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-2019-0680						
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	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-2019-0682 - Windows Subsystem for Linux Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0682 MITRE NVD	**CVE Title:** Windows Subsystem for Linux Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by correcting how Windows Subsystem for Linux handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0682						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Elevation of Privilege	4487020	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Elevation of Privilege	4487020	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	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)	4489886 Security Update	Important	Elevation of Privilege	4486996	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-2019-0682						
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 for x64-based Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 (Server Core Installation)	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 for ARM64-based Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1809 for 32-bit Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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-2019-0682						
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 1809 for ARM64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 2019	4489899 Security Update	Important	Elevation of Privilege	4487044	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 2019 (Server Core installation)	4489899 Security Update	Important	Elevation of Privilege	4487044	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	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-2019-0683 - Active Directory Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0683 MITRE NVD	**CVE Title:** Active Directory Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest. To exploit this vulnerability, an attacker would first need to compromise an Active Directory forest. An attacker who successfully exploited this vulnerability could request delegation of a TGT for an identity from the trusted forest. This update addresses the vulnerability by ensuring Active Directory Forest trusts disable TGT delegation by default. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0683						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Elevation of Privilege	4486563	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0683						
Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Elevation of Privilege	4486563	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4489878 Monthly Rollup 4489885 Security Only	Important	Elevation of Privilege	4486563	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems	4489878 Monthly Rollup 4489885 Security Only	Important	Elevation of Privilege	4486563	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0683						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Elevation of Privilege	4486563	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Elevation of Privilege	4487019	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems	4489880 Monthly Rollup 4489876 Security	Important	Elevation of Privilege	4487019	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0683						
Service Pack 2	Only					
Windows Server 2008 for 32-bit Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Elevation of Privilege	4487019	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Elevation of Privilege	4487019	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server	4489880 Monthly Rollup 4489876 Security Only	Important	Elevation of Privilege	4487019	Base: 4.9 Temporal: 4.4 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0683						
Core installation)						

CVE-2019-0689 - Windows Subsystem for Linux Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0689 MITRE NVD	**CVE Title:** Windows Subsystem for Linux Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by correcting how Windows Subsystem for Linux handles objects in memory. **FAQ:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0689						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709	4489886 Security	Important	Elevation of Privilege	4486996	Base: 7 Temporal: 6.3	Yes

CVE-2019-0689						
for 32-bit Systems	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 1709 for x64-based Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	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)	4489886 Security Update	Important	Elevation of Privilege	4486996	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 1803 for 32-bit Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 for x64-based Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803	4489868 Security Update	Important	Elevation of Privilege	4487017	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-2019-0689						
(Server Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1809 for 32-bit Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 1809 for x64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 1809 for ARM64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 2019	4489899 Security	Important	Elevation of Privilege	4487044	Base: 7 Temporal: 6.3	Yes

CVE-2019-0689						
	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 Server 2019 (Server Core installation)	4489899 Security Update	Important	Elevation of Privilege	4487044	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	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-2019-0690 - Windows Hyper-V Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0690	**CVE Title:** Windows Hyper-V Denial of Service Vulnerability **Description:**	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. An attacker who successfully exploited the vulnerability could cause the host server to crash. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash. The update addresses the vulnerability by modifying how virtual machines access the Hyper-V Network Switch. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0690						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Denial of Service	4486563	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4489878 Monthly Rollup 4489885 Security Only	Important	Denial of Service	4486563	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0690						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Denial of Service	4486563	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Important	Denial of Service	4487025	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Important	Denial of Service	4487025	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0690						
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security Only	Important	Denial of Service	4487000	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Denial of Service	4487000	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2012 R2 (Server Core installation)	4489881 Monthly Rollup 4489883 Security Only	Important	Denial of Service	4487000	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2019-0690						
Windows 10 for x64-based Systems	4489872 Security Update	Important	Denial of Service	4487018	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4489882 Security Update	Important	Denial of Service	4487026	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Denial of Service	4487026	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4489882 Security Update	Important	Denial of Service	4487026	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Denial of Service	4487020	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709	4489886 Security	Important	Denial of Service	4486996	Base: 6.8 Temporal: 6.1	Yes

CVE-2019-0690						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server, version 1709 (Server Core Installation)	4489886 Security Update	Important	Denial of Service	4486996	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Denial of Service	4487017	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Important	Denial of Service	4487017	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Denial of Service	4487044	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security	Important	Denial of Service	4487044	Base: 6.8 Temporal: 6.1	Yes

CVE-2019-0690						
	Update				Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server 2019 (Server Core installation)	4489899 Security Update	Important	Denial of Service	4487044	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Denial of Service	4487019	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Denial of Service	4487019	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0692 - Windows Subsystem for Linux Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0692 MITRE NVD	**CVE Title:** Windows Subsystem for Linux Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by correcting how Windows Subsystem for Linux handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0692						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709	4489886 Security	Important	Elevation of Privilege	4486996	Base: 7 Temporal: 6.3	Yes

CVE-2019-0692						
for x64-based Systems	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 Server, version 1709 (Server Core Installation)	4489886 Security Update	Important	Elevation of Privilege	4486996	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 1803 for 32-bit Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 for x64-based Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 (Server Core Installation)	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 for ARM64-	4489868 Security	Important	Elevation of Privilege	4487017	Base: 7 Temporal: 6.3	Yes

CVE-2019-0692						
based Systems	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 1809 for 32-bit Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 1809 for x64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 1809 for ARM64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 2019	4489899 Security Update	Important	Elevation of Privilege	4487044	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 2019 (Server Core installation)	4489899 Security Update	Important	Elevation of Privilege	4487044	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-2019-0692						
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	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-2019-0693 - Windows Subsystem for Linux Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0693 MITRE NVD	**CVE Title:** Windows Subsystem for Linux Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Windows Subsystem for Linux handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0693						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	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)	4489886 Security Update	Important	Elevation of Privilege	4486996	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 1803 for 32-bit Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 for x64-based Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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-2019-0693						
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 for ARM64-based Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1809 for 32-bit Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 1809 for x64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 1809 for ARM64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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-2019-0693						
Windows Server 2019	4489899 Security Update	Important	Elevation of Privilege	4487044	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 2019 (Server Core installation)	4489899 Security Update	Important	Elevation of Privilege	4487044	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	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-2019-0694 - Windows Subsystem for Linux Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0694 MITRE NVD	**CVE Title:** Windows Subsystem for Linux Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by correcting how Windows Subsystem for Linux handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0694						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709	4489886 Security	Important	Elevation of Privilege	4486996	Base: 7 Temporal: 6.3	Yes

CVE-2019-0694						
for x64-based Systems	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 Server, version 1709 (Server Core Installation)	4489886 Security Update	Important	Elevation of Privilege	4486996	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 1803 for 32-bit Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 for x64-based Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 (Server Core Installation)	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 for ARM64-	4489868 Security	Important	Elevation of Privilege	4487017	Base: 7 Temporal: 6.3	Yes

CVE-2019-0694						
based Systems	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 1809 for 32-bit Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 1809 for x64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 1809 for ARM64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 2019	4489899 Security Update	Important	Elevation of Privilege	4487044	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 2019 (Server Core installation)	4489899 Security Update	Important	Elevation of Privilege	4487044	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-2019-0694						
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	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-2019-0695 - Windows Hyper-V Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0695 MITRE NVD	**CVE Title:** Windows Hyper-V Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by resolving a number of conditions where Hyper-V would fail to prevent a guest operating system from sending malicious requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0695						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for x64-based Systems	4489872 Security Update	Important	Denial of Service	4487018	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4489882 Security Update	Important	Denial of Service	4487026	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Denial of Service	4487026	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4489882 Security Update	Important	Denial of Service	4487026	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Denial of Service	4487020	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0695						
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Denial of Service	4486996	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4489886 Security Update	Important	Denial of Service	4486996	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Denial of Service	4487017	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Important	Denial of Service	4487017	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Denial of Service	4487044	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0695						
Windows Server 2019	4489899 Security Update	Important	Denial of Service	4487044	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4489899 Security Update	Important	Denial of Service	4487044	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0696 - Windows Kernel Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0696 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 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0696						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2016	4489882 Security Update	Important	Elevation of Privilege	4487026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Important	Elevation of Privilege	4487026	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	4489882 Security Update	Important	Elevation of Privilege	4487026	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)	4489882 Security Update	Important	Elevation of Privilege	4487026	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	4489871 Security Update	Important	Elevation of Privilege	4487020	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-2019-0696						
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Elevation of Privilege	4487020	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	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)	4489886 Security Update	Important	Elevation of Privilege	4486996	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 1803 for 32-bit Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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-2019-0696						
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 (Server Core Installation)	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 for ARM64-based Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1809 for 32-bit Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 1809 for x64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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-2019-0696						
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 2019	4489899 Security Update	Important	Elevation of Privilege	4487044	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 2019 (Server Core installation)	4489899 Security Update	Important	Elevation of Privilege	4487044	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	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-2019-0697 - Windows DHCP Client Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0697 MITRE NVD	**CVE Title:** Windows DHCP Client Remote Code Execution Vulnerability **Description:** A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client. An attacker who successfully exploited the vulnerability could run arbitrary code on the client machine. To exploit the vulnerability, an attacker could send a specially crafted DHCP responses to a client. The security update addresses the vulnerability by correcting how Windows DHCP clients handle certain DHCP responses. **FAQ:** None **Mitigations:** None **Workarounds:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0697						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4489868 Security	Critical	Remote Code Execution	4487017	Base: 9.8 Temporal: 8.8	Yes

CVE-2019-0697						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-	4489899 Security	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8	Yes

CVE-2019-0697						
based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0698 - Windows DHCP Client Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0698	**CVE Title:** Windows DHCP Client Remote Code Execution Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client. An attacker who successfully exploited the vulnerability could run arbitrary code on the client machine. To exploit the vulnerability, an attacker could send a specially crafted DHCP responses to a client. The security update addresses the vulnerability by correcting how Windows DHCP clients handle certain DHCP responses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0698						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4489868 Security	Critical	Remote Code Execution	4487017	Base: 9.8 Temporal: 8.8	Yes

CVE-2019-0698						
based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8	Yes

CVE-2019-0698						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	

CVE-2019-0701 - Windows Hyper-V Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0701 MITRE NVD	**CVE Title:** Windows Hyper-V Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application. The security update addresses the vulnerability by resolving a number of conditions where Hyper-V would fail to prevent a guest operating system from sending malicious requests. **FAQ:**	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0701						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0701						
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Denial of Service	4487017	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Important	Denial of Service	4487017	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Denial of Service	4487044	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security Update	Important	Denial of Service	4487044	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4489899 Security Update	Important	Denial of Service	4487044	Base: 6.8 Temporal: 6.1 Vector: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0702 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0702 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. 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 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 update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0702						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0702						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server	4489880 Monthly Rollup 4489876 Security	Important	Information Disclosure	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0702						
Core installation)	Only					
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: N/A Temporal: N/A Vector: N/A	Unknown

CVE-2019-0702						
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Information Disclosure	4487000	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4489881 Monthly Rollup 4489883 Security	Important	Information Disclosure	4487000	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0702						
	Only					
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4489882 Security Update	Important	Information Disclosure	4487026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Important	Information Disclosure	4487026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Information Disclosure	4487026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0702						
Windows Server 2016 (Server Core installation)	4489882 Security Update	Important	Information Disclosure	4487026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Information Disclosure	4487020	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Information Disclosure	4487020	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0702						
Windows Server, version 1709 (Server Core Installation)	4489886 Security Update	Important	Information Disclosure	4486996	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Important	Information Disclosure	4487017	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4489868 Security Update	Important	Information Disclosure	4487017	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0702						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security Update	Important	Information Disclosure	4487044	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security	Important	Information Disclosure	4487044	Base: 5.5 Temporal: 5	Yes

CVE-2019-0702						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0702						
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0703 - Windows SMB Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0703 MITRE NVD	**CVE Title:** Windows SMB Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests. An authenticated attacker who successfully exploited this vulnerability could craft a special packet, which could lead to information disclosure from the server. To exploit the vulnerability, an attacker would have to be able to authenticate and send SMB messages to an impacted Windows SMB Server The security update addresses the vulnerability by correcting how Windows SMB Server handles authenticated requests. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0703						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0703						
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0703						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0703						
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 8.1 for x64-	4489881 Monthly	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9	Unknown

CVE-2019-0703						
based systems	Rollup 4489883 Security Only				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0703						
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4489882 Security Update	Important	Information Disclosure	4487026	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Important	Information Disclosure	4487026	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Information Disclosure	4487026	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4489882 Security	Important	Information Disclosure	4487026	Base: 6.5 Temporal: 5.9	Yes

CVE-2019-0703						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Information Disclosure	4487020	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Information Disclosure	4487020	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version	4489886 Security	Important	Information Disclosure	4486996	Base: 6.5 Temporal: 5.9	Yes

CVE-2019-0703						
1709 (Server Core Installation)	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Important	Information Disclosure	4487017	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4489868 Security Update	Important	Information Disclosure	4487017	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0703						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security Update	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9	Yes

CVE-2019-0703						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0703						
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0704 - Windows SMB Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0704 MITRE NVD	**CVE Title:** Windows SMB Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests. An authenticated attacker who successfully exploited this vulnerability could craft a special packet, which could lead to information disclosure from the server. To exploit the vulnerability, an attacker would have to be able to authenticate and send SMB messages to an impacted Windows SMB Server The security update addresses the vulnerability by correcting how Windows SMB Server handles authenticated requests. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0704						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0704						
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0704						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0704						
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 8.1 for x64-	4489881 Monthly	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9	Unknown

CVE-2019-0704						
based systems	Rollup 4489883 Security Only				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0704						
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4489882 Security Update	Important	Information Disclosure	4487026	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Important	Information Disclosure	4487026	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Information Disclosure	4487026	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4489882 Security	Important	Information Disclosure	4487026	Base: 6.5 Temporal: 5.9	Yes

CVE-2019-0704						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Information Disclosure	4487020	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Information Disclosure	4487020	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version	4489886 Security	Important	Information Disclosure	4486996	Base: 6.5 Temporal: 5.9	Yes

CVE-2019-0704						
1709 (Server Core Installation)	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Important	Information Disclosure	4487017	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4489868 Security Update	Important	Information Disclosure	4487017	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0704						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security Update	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9	Yes

CVE-2019-0704						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0704						
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0726 - Windows DHCP Client Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0726 MITRE NVD	**CVE Title:** Windows DHCP Client Remote Code Execution Vulnerability **Description:** A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client. An attacker who successfully exploited the vulnerability could run arbitrary code on the client machine. To exploit the vulnerability, an attacker could send a specially crafted DHCP responses to a client. The security update addresses the vulnerability by correcting how Windows DHCP clients handle certain DHCP responses. **FAQ:** None **Mitigations:** None **Workarounds:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0726						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803	4489868 Security	Critical	Remote Code Execution	4487017	Base: 9.8 Temporal: 8.8	Yes

CVE-2019-0726						
for x64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-	4489899 Security	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8	Yes

CVE-2019-0726						
based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2019	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 9.8 Temporal: 8.8 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0746 - Chakra Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0746 MITRE NVD	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

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

CVE-2019-0746						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems	4489880 Monthly Rollup 4489873 IE Cumulative	Low	Remote Code Execution	4486474	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-2019-0746						
Service Pack 2						
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489873 IE Cumulative	Low	Remote Code Execution	4486474	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	4489878 Monthly Rollup 4489873 IE Cumulative	Important	Remote Code Execution	4486474	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	4489878 Monthly Rollup	Important	Remote Code Execution	4486474	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0746						
Windows 7 for x64-based Systems Service Pack 1	4489873 IE Cumulative				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 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Low	Remote Code Execution	4486474	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	4489873 IE Cumulative 4489881 Monthly Rollup	Important	Remote Code Execution	4487000	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-2019-0746						
Internet Explorer 11 on Windows 8.1 for x64-based systems	4489873 IE Cumulative 4489881 Monthly Rollup	Important	Remote Code Execution	4487000	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	4489873 IE Cumulative 4489881 Monthly Rollup	Low	Remote Code Execution	4487000	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	4489881 Monthly Rollup	Important	Remote Code Execution	4487000	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	4489872 Security Update	Important	Remote Code Execution	4487018	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-2019-0746						
10 for 32-bit Systems						
Internet Explorer 11 on Windows 10 for x64-based Systems	4489872 Security Update	Important	Remote Code Execution	4487018	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	4489882 Security Update	Low	Remote Code Execution	4487026	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	4489882 Security Update	Important	Remote Code Execution	4487026	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-2019-0746						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Remote Code Execution	4487026	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	4489871 Security Update	Important	Remote Code Execution	4487020	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	4489871 Security Update	Important	Remote Code Execution	4487020	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-2019-0746						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	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	4489868 Security Update	Important	Remote Code Execution	4487017	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-2019-0746						
1803 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	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 1803 for ARM64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	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	4489899 Security	Important	Remote Code Execution	4487044	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0746						
Windows 10 Version 1809 for 32-bit Systems	Update				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 1809 for x64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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 1809 for ARM64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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-2019-0746						
Internet Explorer 11 on Windows Server 2019	4489899 Security Update	Low	Remote Code Execution	4487044	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 1709 for ARM64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 10 on Windows Server 2012	4489873 IE Cumulative 4489891 Monthly Rollup	Low	Remote Code Execution	4487025	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-2019-0746						
Microsoft Edge on Windows 10 for 32-bit Systems	4489872 Security Update	Important	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489872 Security Update	Important	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Low	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Important	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0746						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489871 Security Update	Important	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489871 Security Update	Important	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0746						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for 32-bit Systems	4489868 Security Update	Important	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0746						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for ARM64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for 32-bit Systems	4489899 Security Update	Important	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0746						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for ARM64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 2019	4489899 Security Update	Low	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4489886 Security	Important	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0746						
10 Version 1709 for ARM64-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	
ChakraCore	Release Notes Security Update	Important	Remote Code Execution	4486996	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0748 - Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0748	**CVE Title:** Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory. An attacker who successfully exploited this vulnerability could execute arbitrary code on a victim system. An attacker could exploit this vulnerability by enticing a victim to open a specially crafted file. The update addresses the vulnerability by correcting the way the Microsoft Office Access Connectivity Engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0748						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4462226 Security Update	Important	Remote Code Execution	4018313	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4462226 Security Update	Important	Remote Code Execution	4018313	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0754 - Windows Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0754 MITRE NVD	**CVE Title:** Windows Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Windows improperly handles objects in memory. An attacker who successfully exploited the vulnerability could cause a target system to stop responding. 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 cause a target system to stop responding. The update addresses the vulnerability by correcting how Windows handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0754						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Denial of Service	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0754						
Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Denial of Service	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/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)	4489878 Monthly Rollup 4489885 Security Only	Important	Denial of Service	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Denial of Service	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0754						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Denial of Service	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/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)	4489880 Monthly Rollup 4489876 Security Only	Important	Denial of Service	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Important	Denial of Service	4487025	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0754						
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Important	Denial of Service	4487025	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4489881 Monthly Rollup 4489883 Security Only	Important	Denial of Service	4487000	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security Only	Important	Denial of Service	4487000	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown

CVE-2019-0754						
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Denial of Service	4487000	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Denial of Service	4487000	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4489881 Monthly Rollup 4489883 Security Only	Important	Denial of Service	4487000	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Unknown
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Denial of Service	4487018	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0754						
Windows 10 for x64-based Systems	4489872 Security Update	Important	Denial of Service	4487018	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4489882 Security Update	Important	Denial of Service	4487026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/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	4489882 Security Update	Important	Denial of Service	4487026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Denial of Service	4487026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4489882 Security Update	Important	Denial of Service	4487026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703	4489871 Security	Important	Denial of Service	4487020	Base: 5.5 Temporal: 5	Yes

CVE-2019-0754						
for 32-bit Systems	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Denial of Service	4487020	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Denial of Service	4486996	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Denial of Service	4486996	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4489886 Security Update	Important	Denial of Service	4486996	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Denial of Service	4487017	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0754						
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Denial of Service	4487017	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Important	Denial of Service	4487017	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Important	Denial of Service	4487017	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Denial of Service	4487044	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Denial of Service	4487044	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0754						
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Denial of Service	4487044	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security Update	Important	Denial of Service	4487044	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2019 (Server Core installation)	4489899 Security Update	Important	Denial of Service	4487044	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Denial of Service	4486996	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Denial of Service	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0754						
Windows Server 2008 for 32-bit Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Denial of Service	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/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	4489880 Monthly Rollup 4489876 Security Only	Important	Denial of Service	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/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 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Denial of Service	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2019-0755 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0755 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. 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 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 update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0755						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0755						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server	4489880 Monthly Rollup 4489876 Security	Important	Information Disclosure	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0755						
Core installation)	Only					
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0755						
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Information Disclosure	4487000	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4489881 Monthly Rollup 4489883 Security	Important	Information Disclosure	4487000	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0755						
	Only					
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4489882 Security Update	Important	Information Disclosure	4487026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Important	Information Disclosure	4487026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Information Disclosure	4487026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0755						
Windows Server 2016 (Server Core installation)	4489882 Security Update	Important	Information Disclosure	4487026	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Information Disclosure	4487020	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Information Disclosure	4487020	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0755						
Windows Server, version 1709 (Server Core Installation)	4489886 Security Update	Important	Information Disclosure	4486996	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Important	Information Disclosure	4487017	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for ARM64-	4489868 Security Update	Important	Information Disclosure	4487017	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0755						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security Update	Important	Information Disclosure	4487044	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security	Important	Information Disclosure	4487044	Base: 5.5 Temporal: 5	Yes

CVE-2019-0755						
(Server Core installation)	Update				Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0755						
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0756 - MS XML Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0756 MITRE NVD	**CVE Title:** MS XML Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input. An attacker who successfully exploited the vulnerability could run malicious code remotely to take control of the userâ€™s system. To exploit the vulnerability, an attacker could host a specially crafted website designed to invoke MSXML through a web browser. However, an attacker would have no way to force a user to visit such a website. Instead, an attacker would typically have to convince a user to either click a link in an email message or instant message that would then take the user to the website. When Internet Explorer parses the XML content, an attacker could run malicious code remotely to take control of the userâ€™s system. The update addresses the vulnerability by correcting how the MSXML parser processes user input. **FAQ:** None **Mitigations:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0756						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4489878 Monthly Rollup 4489885	Critical	Remote Code Execution	4486563	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-2019-0756						
Service Pack 1	Security Only					
Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Critical	Remote Code Execution	4486563	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
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4489878 Monthly Rollup 4489885 Security Only	Critical	Remote Code Execution	4486563	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
Windows Server 2008 R2 for Itanium-	4489878 Monthly Rollup 4489885	Critical	Remote Code Execution	4486563	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-2019-0756						
Based Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Critical	Remote Code Execution	4486563	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
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Critical	Remote Code Execution	4487019	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
Windows Server 2012	4489884 Security Only 4489891	Critical	Remote Code Execution	4487025	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-2019-0756						
	Monthly Rollup					
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Critical	Remote Code Execution	4487025	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
Windows 8.1 for 32-bit systems	4489881 Monthly Rollup 4489883 Security Only	Critical	Remote Code Execution	4487000	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	Unknown
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security	Critical	Remote Code Execution	4487000	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	Unknown

CVE-2019-0756						
	Only					
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Critical	Remote Code Execution	4487000	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	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	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
Windows Server 2012 R2 (Server Core installation)	4489881 Monthly Rollup 4489883 Security Only	Critical	Remote Code Execution	4487000	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	Unknown
Windows 10 for 32-bit Systems	4489872 Security	Critical	Remote Code Execution	4487018	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0756						
	Update				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	
Windows 10 for x64-based Systems	4489872 Security Update	Critical	Remote Code Execution	4487018	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
Windows Server 2016	4489882 Security Update	Critical	Remote Code Execution	4487026	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
Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Critical	Remote Code Execution	4487026	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
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Critical	Remote Code Execution	4487026	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
Windows Server 2016 (Server Core installation)	4489882 Security Update	Critical	Remote Code Execution	4487026	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-2019-0756						
Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Critical	Remote Code Execution	4487020	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
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Critical	Remote Code Execution	4487020	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
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	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
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	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
Windows Server, version 1709 (Server Core Installation)	4489886 Security Update	Critical	Remote Code Execution	4486996	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-2019-0756						
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	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
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	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
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Critical	Remote Code Execution	4487017	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
Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	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
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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-2019-0756						
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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
Windows Server 2019	4489899 Security Update	Critical	Remote Code Execution	4487044	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
Windows Server 2019 (Server Core installation)	4489899 Security Update	Critical	Remote Code Execution	4487044	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
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	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-2019-0756						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Critical	Remote Code Execution	4487019	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
Windows Server 2008 for 32-bit Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Critical	Remote Code Execution	4487019	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
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Critical	Remote Code Execution	4487019	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-2019-0756						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Critical	Remote Code Execution	4487019	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-2019-0757 - NuGet Package Manager Tampering Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0757 MITRE NVD	**CVE Title:** NuGet Package Manager Tampering Vulnerability **Description:** A tampering vulnerability exists in the NuGet Package Manager for Linux and Mac that could allow an authenticated attacker to modify a NuGet package's folder structure. An attacker who successfully exploited this vulnerability could potentially modify files and folders that are unpackaged on a system.	Important	Tampering

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit this vulnerability, an attacker would need to log on to the affected system and tamper with the folder contents of a package prior to building or installation of an application. The security update addresses the vulnerability by correcting permissions on folders inside the NuGet packages folder structure. **FAQ:** **Is there any additional information I need to apply the updates?** Yes. To apply the updates, follow step A1 or A2, and then step B. A1. Delete all NuGet package extraction folders, including all global packages folder(s) and solution packages folger(s). A2. Apply the workaround described in the Workaround section on the existing folders and any files in the package extraction folders. B. Install and use the updates. **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	This issue can be worked around if you change the directory permissions of all NuGet package extraction locations on your computer. These locations generally will include a global package folder (defaults to ~/.nuget/packages, but overridable by nuget.config settings). If any of your projects use packages.config for NuGet, each of the containing solutions will also have a solution packages folder. To change directory permissions so only the current user can access the default location of the global packages folder: chmod -R go-wx ~/.nuget/packages **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0757						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Visual Studio for Mac	Release Notes Security Update	Important	Tampering		Base: N/A Temporal: N/A Vector: N/A	Maybe
.NET Core SDK 1.1 on .NET Core 1.0	Release Notes Security Update	Important	Tampering		Base: N/A Temporal: N/A Vector: N/A	Maybe
.NET Core SDK 2.1.500	Release Notes Security Update	Important	Tampering		Base: N/A Temporal: N/A Vector: N/A	Maybe
.NET Core SDK 1.1 on .NET Core 1.1	Release Notes Security Update	Important	Tampering		Base: N/A Temporal: N/A Vector: N/A	Maybe
Nuget 4.3.1	Release Notes Security Update	Important	Tampering		Base: N/A Temporal: N/A Vector: N/A	Maybe
Nuget 4.4.2	Release Notes Security Update	Important	Tampering		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0757						
Nuget 4.5.2	Release Notes Security Update	Important	Tampering		Base: N/A Temporal: N/A Vector: N/A	Maybe
Nuget 4.6.3	Release Notes Security Update	Important	Tampering		Base: N/A Temporal: N/A Vector: N/A	Maybe
Nuget 4.7.2	Release Notes Security Update	Important	Tampering		Base: N/A Temporal: N/A Vector: N/A	Maybe
Nuget 4.8.2	Release Notes Security Update	Important	Tampering		Base: N/A Temporal: N/A Vector: N/A	Maybe
Nuget 4.9.4	Release Notes Security Update	Important	Tampering		Base: N/A Temporal: N/A Vector: N/A	Maybe
Mono Framework Version 5.18.0.223	Release Notes Security Update	Important	Tampering		Base: N/A Temporal: N/A Vector: N/A	Maybe
Mono Framework Version 5.20.0	Release Notes Security Update	Important	Tampering		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0759 - Windows Print Spooler Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0759 MITRE NVD	**CVE Title:** Windows Print Spooler Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows Print Spooler does not properly handle objects in memory. An attacker who successfully exploited this vulnerability could use the information to further exploit the victim system. To exploit this vulnerability, an attacker would have to first gain execution on the victim system. The update addresses the vulnerability by correcting how the Windows Print Spooler handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0759						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit	4489878 Monthly	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0759						
Systems Service Pack 1	Rollup 4489885 Security Only				Vector: CVSS: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	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489878 Monthly	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0759						
R2 for Itanium-Based Systems Service Pack 1	Rollup 4489885 Security Only				Vector: CVSS: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	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489884 Security	Important	Information Disclosure	4487025	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0759						
	Only 4489891 Monthly Rollup				Vector: CVSS: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)	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0759						
	Security Only					
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0759						
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489872 Security Update	Important	Information Disclosure	4487018	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0759						
(Server Core installation)	Update				Vector: CVSS: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 1703 for 32-bit Systems	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489886 Security	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0759						
1709 (Server Core Installation)	Update				Vector: CVSS: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 1803 for 32-bit Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 for x64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 (Server Core Installation)	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 for ARM64-	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0759						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1809 for x64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1809 for ARM64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 2019	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 2019	4489899 Security	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0759						
(Server Core installation)	Update				Vector: CVSS: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 ARM64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0759						
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0761 - Internet Explorer Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0761 MITRE NVD	**CVE Title:** Internet Explorer Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Internet Explorer fails to validate the correct Security Zone of requests for specific URLs. This could allow an attacker to cause a user to access a URL in a less restricted Internet Security Zone than intended. To exploit this vulnerability, an attacker could email or otherwise provide a specially crafted URL to a victim and convince them to click on it. The security update addresses the vulnerability by correcting security feature behavior to properly map affected URLs to the correct Security Zone. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00	Low	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

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

CVE-2019-0761						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Important	Security Feature Bypass	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Important	Security Feature Bypass	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0761						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Low	Security Feature Bypass	4486474	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4489873 IE Cumulative 4489881 Monthly Rollup	Important	Security Feature Bypass	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4489873 IE Cumulative 4489881 Monthly Rollup	Important	Security Feature Bypass	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows Server 2012 R2	4489873 IE Cumulative 4489881 Monthly Rollup	Low	Security Feature Bypass	4487000	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows RT 8.1	4489881 Monthly Rollup	Important	Security Feature Bypass	4487000	Base: N/A Temporal:	Yes

CVE-2019-0761						
					N/A Vector: N/A	
Internet Explorer 11 on Windows 10 for 32-bit Systems	4489872 Security Update	Important	Security Feature Bypass	4487018	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4489872 Security Update	Important	Security Feature Bypass	4487018	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows Server 2016	4489882 Security Update	Low	Security Feature Bypass	4487026	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Important	Security Feature Bypass	4487026	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Security Feature Bypass	4487026	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0761						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Security Feature Bypass	4487020	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Security Feature Bypass	4487020	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Security Feature Bypass	4486996	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Security Feature Bypass	4486996	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Security Feature Bypass	4487017	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Security Feature Bypass	4487017	Base: N/A Temporal:	Yes

CVE-2019-0761						
					N/A Vector: N/A	
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Important	Security Feature Bypass	4487017	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Security Feature Bypass	4487044	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Security Feature Bypass	4487044	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Security Feature Bypass	4487044	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 11 on Windows Server 2019	4489899 Security Update	Low	Security Feature Bypass	4487044	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0761						
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Security Feature Bypass	4486996	Base: N/A Temporal: N/A Vector: N/A	Yes
Internet Explorer 10 on Windows Server 2012	4489873 IE Cumulative 4489891 Monthly Rollup	Low	Security Feature Bypass	4487025	Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0762 - Microsoft Browsers Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0762 MITRE NVD	**CVE Title:** Microsoft Browsers Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Microsoft browsers improperly handle requests of different origins. The vulnerability allows Microsoft browsers to bypass Same-Site cookie restrictions, and to allow requests that should otherwise be ignored. An attacker who	Low	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	successfully exploited the vulnerability could force the browser to send data that would otherwise be restricted. In a web-based attack scenario, 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, 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 browsers handle cross-domain requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0762						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Important	Security Feature Bypass	4486474	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	4489878 Monthly Rollup 4489873 IE Cumulative	Important	Security Feature Bypass	4486474	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-2019-0762						
Service Pack 1						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Low	Security Feature Bypass	4486474	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	4489873 IE Cumulative 4489881 Monthly Rollup	Important	Security Feature Bypass	4487000	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-	4489873 IE Cumulative 4489881 Monthly	Important	Security Feature Bypass	4487000	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-2019-0762						
based systems	Rollup					
Internet Explorer 11 on Windows Server 2012 R2	4489873 IE Cumulative 4489881 Monthly Rollup	Low	Security Feature Bypass	4487000	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	4489881 Monthly Rollup	Important	Security Feature Bypass	4487000	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Security Feature Bypass	4486996	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	4489886 Security	Important	Security Feature Bypass	4486996	Base: 4.3 Temporal: 3.9	Yes

CVE-2019-0762						
Windows 10 Version 1709 for x64-based Systems	Update				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	
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Security Feature Bypass	4487017	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 1803 for x64-based Systems	4489868 Security Update	Important	Security Feature Bypass	4487017	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	4489868 Security	Important	Security Feature Bypass	4487017	Base: 4.3 Temporal: 3.9	Yes

CVE-2019-0762						
Windows 10 Version 1803 for ARM64-based Systems	Update				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	
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Security Feature Bypass	4487044	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 1809 for x64-based Systems	4489899 Security Update	Important	Security Feature Bypass	4487044	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-2019-0762						
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Security Feature Bypass	4487044	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 2019	4489899 Security Update	Low	Security Feature Bypass	4487044	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 1709 for ARM64-based Systems	4489886 Security Update	Important	Security Feature Bypass	4486996	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-2019-0762						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Security Feature Bypass	4486996	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/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 x64-based Systems	4489886 Security Update	Important	Security Feature Bypass	4486996	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/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 1803 for 32-bit Systems	4489868 Security Update	Important	Security Feature Bypass	4487017	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/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	4489868 Security Update	Important	Security Feature Bypass	4487017	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0762						
1803 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Important	Security Feature Bypass	4487017	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/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 1809 for 32-bit Systems	4489899 Security Update	Important	Security Feature Bypass	4487044	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/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 1809 for	4489899 Security Update	Important	Security Feature Bypass	4487044	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0762						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Security Feature Bypass	4487044	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2019	4489899 Security Update	Low	Security Feature Bypass	4487044	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/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 ARM64-based Systems	4489886 Security Update	Important	Security Feature Bypass	4486996	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0763 - Internet Explorer Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0763 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 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.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0763						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Critical	Remote Code Execution	4486474	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	4489878 Monthly Rollup 4489873 IE Cumulative	Critical	Remote Code Execution	4486474	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	4489878 Monthly Rollup	Moderate	Remote Code Execution	4486474	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-0763						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489873 IE Cumulative				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	
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4489873 IE Cumulative 4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	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	4489873 IE Cumulative 4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	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-2019-0763						
Internet Explorer 11 on Windows Server 2012 R2	4489873 IE Cumulative 4489881 Monthly Rollup	Moderate	Remote Code Execution	4487000	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	4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	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	4489872 Security Update	Critical	Remote Code Execution	4487018	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	4489872 Security Update	Critical	Remote Code Execution	4487018	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-2019-0763						
x64-based Systems						
Internet Explorer 11 on Windows Server 2016	4489882 Security Update	Moderate	Remote Code Execution	4487026	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	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4489882 Security Update	Critical	Remote Code Execution	4487026	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-2019-0763						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Critical	Remote Code Execution	4487020	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	4489871 Security Update	Critical	Remote Code Execution	4487020	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	4489886 Security Update	Critical	Remote Code Execution	4486996	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-2019-0763						
1709 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	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 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	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	4489868 Security Update	Critical	Remote Code Execution	4487017	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-2019-0763						
10 Version 1803 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	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 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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-2019-0763						
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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 1809 for ARM64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	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 2019	4489899 Security Update	Moderate	Remote Code Execution	4487044	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-2019-0763						
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 10 on Windows Server 2012	4489873 IE Cumulative 4489891 Monthly Rollup	Moderate	Remote Code Execution	4487025	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-2019-0765 - Comctl32 Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0765 MITRE NVD	**CVE Title:** Comctl32 Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, 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.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by modifying how comctl32.dll handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0765						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Remote Code Execution	4486563	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
Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Remote Code Execution	4486563	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
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server	4489878 Monthly Rollup 4489885 Security Only	Important	Remote Code Execution	4486563	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-2019-0765						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Remote Code Execution	4486563	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
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Remote Code Execution	4486563	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
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server	4489880 Monthly Rollup 4489876 Security	Important	Remote Code Execution	4487019	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-2019-0765						
Core installation)	Only					
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Important	Remote Code Execution	4487025	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
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Important	Remote Code Execution	4487025	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
Windows 8.1 for 32-bit systems	4489881 Monthly Rollup 4489883 Security Only	Important	Remote Code Execution	4487000	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	Unknown

CVE-2019-0765						
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security Only	Important	Remote Code Execution	4487000	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	Unknown
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Remote Code Execution	4487000	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	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Remote Code Execution	4487000	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
Windows Server 2012 R2 (Server Core installation)	4489881 Monthly Rollup 4489883 Security	Important	Remote Code Execution	4487000	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	Unknown

CVE-2019-0765						
	Only					
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Remote Code Execution	4487018	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
Windows 10 for x64-based Systems	4489872 Security Update	Important	Remote Code Execution	4487018	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
Windows Server 2016	4489882 Security Update	Important	Remote Code Execution	4487026	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
Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Important	Remote Code Execution	4487026	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
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Remote Code Execution	4487026	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-2019-0765						
Windows Server 2016 (Server Core installation)	4489882 Security Update	Important	Remote Code Execution	4487026	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
Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Remote Code Execution	4487020	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
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Remote Code Execution	4487020	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
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Remote Code Execution	4486996	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
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	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-2019-0765						
Windows Server, version 1709 (Server Core Installation)	4489886 Security Update	Important	Remote Code Execution	4486996	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
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Remote Code Execution	4487017	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
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	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
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Important	Remote Code Execution	4487017	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
Windows 10 Version 1803 for ARM64-	4489868 Security Update	Important	Remote Code Execution	4487017	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-2019-0765						
based Systems						
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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
Windows Server 2019	4489899 Security Update	Important	Remote Code Execution	4487044	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
Windows Server 2019	4489899 Security	Important	Remote Code Execution	4487044	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-0765						
(Server Core installation)	Update				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	
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	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
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Remote Code Execution	4487019	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
Windows Server 2008 for 32-bit Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Remote Code Execution	4487019	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-2019-0765						
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Remote Code Execution	4487019	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
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Remote Code Execution	4487019	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-2019-0766 - Microsoft Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0766 MITRE NVD	**CVE Title:** Microsoft Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows AppX Deployment Server that allows file creation in arbitrary locations. To exploit the vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by not permitting Windows AppX Deployment Server to create files in arbitrary locations. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Information published.		

Affected Software

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

CVE-2019-0766						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2016	4489882 Security Update	Important	Elevation of Privilege	4487026	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Important	Elevation of Privilege	4487026	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes

CVE-2019-0766						
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Elevation of Privilege	4487026	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows Server 2016 (Server Core installation)	4489882 Security Update	Important	Elevation of Privilege	4487026	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Elevation of Privilege	4487020	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Elevation of Privilege	4487020	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security	Important	Elevation of Privilege	4486996	Base: 6.7 Temporal: 6.7	Yes

CVE-2019-0766						
	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	
Windows Server, version 1709 (Server Core Installation)	4489886 Security Update	Important	Elevation of Privilege	4486996	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Important	Elevation of Privilege	4487017	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes

CVE-2019-0766						
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows Server 2019	4489899 Security Update	Important	Elevation of Privilege	4487044	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows Server 2019 (Server Core installation)	4489899 Security Update	Important	Elevation of Privilege	4487044	Base: 6.7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security	Important	Elevation of Privilege	4486996	Base: 6.7 Temporal: 6.7	Yes

CVE-2019-0766						
	Update				Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	

CVE-2019-0767 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0767 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. The update addresses the vulnerability by correcting how the Windows kernel initializes objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory and kernel memory - unintentional read access to memory contents in kernel space from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0767						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0767						
(Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489880 Monthly Rollup 4489876 Security	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0767						
(Server Core installation)	Only					
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0767						
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489881 Monthly Rollup 4489883 Security	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0767						
	Only					
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489872 Security Update	Important	Information Disclosure	4487018	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0767						
Windows Server 2016 (Server Core installation)	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0767						
Windows Server, version 1709 (Server Core Installation)	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 for 32-bit Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 for x64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 (Server Core Installation)	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489868 Security	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0767						
1803 for ARM64-based Systems	Update				Vector: CVSS: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 1809 for 32-bit Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1809 for x64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1809 for ARM64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 2019	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0767						
Windows Server 2019 (Server Core installation)	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 ARM64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489880 Monthly Rollup 4489876 Security	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0767						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0768 - Internet Explorer Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0768 MITRE NVD	**CVE Title:** Internet Explorer Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Internet Explorer VBScript execution policy does not properly restrict VBScript under specific conditions, and to allow 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. In a web-based attack scenario, an attacker could host a website in an attempt to exploit this vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. The update addresses the vulnerability by fixing how the Internet Explorer VBScript execution policy validates embedded VBScript content. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0768						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Security Feature Bypass	4486996	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-2019-0768						
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Security Feature Bypass	4486996	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 1803 for 32-bit Systems	4489868 Security Update	Important	Security Feature Bypass	4487017	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 1803 for x64-based Systems	4489868 Security Update	Important	Security Feature Bypass	4487017	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	4489868 Security	Important	Security Feature Bypass	4487017	Base: 4.3 Temporal: 3.9	Yes

CVE-2019-0768						
10 Version 1803 for ARM64-based Systems	Update				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	
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Security Feature Bypass	4487044	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 1809 for x64-based Systems	4489899 Security Update	Important	Security Feature Bypass	4487044	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 1809 for	4489899 Security Update	Important	Security Feature Bypass	4487044	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-2019-0768						
ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4489899 Security Update	Low	Security Feature Bypass	4487044	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 1709 for ARM64-based Systems	4489886 Security Update	Important	Security Feature Bypass	4486996	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-2019-0769 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0769 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 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0769						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0769						
Microsoft Edge on Windows 10 for 32-bit Systems	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Moderate	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security	Critical	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0769						
Version 1607 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 1703 for 32-bit Systems	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0769						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for x64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for ARM64-	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0769						
based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for ARM64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0769						
Microsoft Edge on Windows Server 2019	4489899 Security Update	Moderate	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 ARM64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4486996	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0770 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0770 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 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0770						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0770						
Microsoft Edge on Windows 10 for 32-bit Systems	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Moderate	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0770						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489886 Security	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0770						
Version 1709 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 1709 for x64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for x64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0770						
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 ARM64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0771 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0771 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 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0771						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0771						
Microsoft Edge on Windows 10 for 32-bit Systems	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Moderate	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security	Critical	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0771						
Version 1607 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 1703 for 32-bit Systems	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0771						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for x64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for ARM64-	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0771						
based Systems						
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for ARM64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0771						
Microsoft Edge on Windows Server 2019	4489899 Security Update	Moderate	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 ARM64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0772 - Windows VBScript Engine Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0772 MITRE NVD	**CVE Title:** Windows VBScript Engine Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0772						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Remote Code Execution	4486563	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	Yes
Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Remote Code Execution	4486563	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	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4489878 Monthly Rollup 4489885 Security Only	Important	Remote Code Execution	4486563	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	Yes

CVE-2019-0772						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Remote Code Execution	4486563	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	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Remote Code Execution	4486563	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	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Remote Code Execution	4487019	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	Yes

CVE-2019-0772						
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Important	Remote Code Execution	4487025	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	Yes
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Important	Remote Code Execution	4487025	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	Yes
Windows 8.1 for 32-bit systems	4489881 Monthly Rollup 4489883 Security Only	Important	Remote Code Execution	4487000	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	Unknown

CVE-2019-0772						
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security Only	Important	Remote Code Execution	4487000	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	Unknown
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Remote Code Execution	4487000	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	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Remote Code Execution	4487000	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	Yes
Windows Server 2012 R2 (Server Core installation)	4489881 Monthly Rollup 4489883 Security	Important	Remote Code Execution	4487000	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	Unknown

CVE-2019-0772						
	Only					
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Remote Code Execution	4487018	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	Yes
Windows 10 for x64-based Systems	4489872 Security Update	Important	Remote Code Execution	4487018	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	Yes
Windows Server 2016	4489882 Security Update	Important	Remote Code Execution	4487026	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	Yes
Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Important	Remote Code Execution	4487026	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	Yes
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Remote Code Execution	4487026	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	Yes

CVE-2019-0772						
Windows Server 2016 (Server Core installation)	4489882 Security Update	Important	Remote Code Execution	4487026	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	Yes
Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Remote Code Execution	4487020	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	Yes
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Remote Code Execution	4487020	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	Yes
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Remote Code Execution	4486996	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	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	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	Yes
Windows Server, version 1709	4489886 Security	Important	Remote Code Execution	4486996	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-0772						
(Server Core Installation)	Update				Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Remote Code Execution	4487017	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	Yes
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	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	Yes
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Important	Remote Code Execution	4487017	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	Yes
Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	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	Yes
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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	Yes

CVE-2019-0772						
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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	Yes
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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	Yes
Windows Server 2019	4489899 Security Update	Important	Remote Code Execution	4487044	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	Yes
Windows Server 2019 (Server Core installation)	4489899 Security Update	Important	Remote Code Execution	4487044	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	Yes
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	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	Yes
Windows Server 2008 for Itanium-Based	4489880 Monthly Rollup	Important	Remote Code Execution	4487019	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-0772						
Systems Service Pack 2	4489876 Security Only				Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O	
Windows Server 2008 for 32-bit Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Remote Code Execution	4487019	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	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Remote Code Execution	4487019	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	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security	Important	Remote Code Execution	4487019	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	Yes

CVE-2019-0772						
(Server Core installation)	Only					

CVE-2019-0773 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0773 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0773						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Moderate	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0773						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0773						
for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for x64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489868 Security	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0773						
Version 1803 for ARM64-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 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for ARM64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0773						
Microsoft Edge on Windows Server 2019	4489899 Security Update	Moderate	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 ARM64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Release Notes Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Maybe

CVE-2019-0774 - Windows GDI Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0774 MITRE NVD	**CVE Title:** Windows GDI Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage. The security update addresses the vulnerability by correcting how the Windows GDI component handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0774						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems	4489878 Monthly Rollup 4489885	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0774						
Service Pack 1	Security Only					
Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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-	4489878 Monthly Rollup 4489885	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0774						
Based Systems Service Pack 1	Security Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489884 Security Only 4489891	Important	Information Disclosure	4487025	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0774						
	Monthly Rollup					
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0774						
	Only					
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 for 32-bit Systems	4489872 Security	Important	Information Disclosure	4487018	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0774						
	Update				Vector: CVSS: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 for x64-based Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0774						
Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0774						
(Server Core Installation)						
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 for x64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 (Server Core Installation)	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 for ARM64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0774						
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1809 for x64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1809 for ARM64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 2019	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 2019 (Server Core installation)	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0774						
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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-	4489880 Monthly Rollup	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0774						
based Systems Service Pack 2	4489876 Security Only				Vector: CVSS: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 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0775 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0775 MITRE NVD	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. 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 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 update addresses the vulnerability by correcting how the Windows kernel handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process. **Mitigations:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0775						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0775						
	Only					
Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489878 Monthly Rollup 4489885 Security	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0775						
Systems Service Pack 1	Only					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489884 Security Only 4489891 Monthly	Important	Information Disclosure	4487025	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0775						
	Rollup					
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0775						
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0775						
Windows 10 for x64-based Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489871 Security	Important	Information Disclosure	4487020	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0775						
1703 for 32-bit Systems	Update				Vector: CVSS: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 1703 for x64-based Systems	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0775						
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 for x64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 (Server Core Installation)	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 for ARM64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489899 Security	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0775						
1809 for 32-bit Systems	Update				Vector: CVSS: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 1809 for x64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1809 for ARM64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 2019	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 2019 (Server Core installation)	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489886 Security	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0775						
1709 for ARM64-based Systems	Update				Vector: CVSS: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	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489880 Monthly Rollup 4489876 Security	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0775						
Service Pack 2	Only					
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0776 - Win32k Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0776 MITRE NVD	**CVE Title:** Win32k Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the win32k component improperly provides kernel information. 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
	To exploit the vulnerability, an attacker would have to either log on locally to an affected system, or convince a locally authenticated user to execute a specially crafted application. The security update addresses the vulnerability by correcting how win32k handles objects in memory. **FAQ:** **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is Kernel memory read - unintentional read access to memory contents in kernel space from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0776						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489872 Security Update	Important	Information Disclosure	4487018	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0776						
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0776						
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 for 32-bit Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 for x64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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,	4489868 Security	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0776						
version 1803 (Server Core Installation)	Update				Vector: CVSS: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 1803 for ARM64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1809 for 32-bit Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1809 for x64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1809 for	4489899 Security	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0776						
ARM64-based Systems	Update				Vector: CVSS: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 2019	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 2019 (Server Core installation)	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 ARM64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0777 - Team Foundation Server Cross-site Scripting Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0777 MITRE NVD	**CVE Title:** Team Foundation Server Cross-site Scripting Vulnerability **Description:** A Cross-site Scripting (XSS) vulnerability exists when Team Foundation Server does not properly sanitize user provided input. An authenticated attacker could exploit the vulnerability by sending a specially crafted payload to the Team Foundation Server, which will get executed in the context of the user every time a user visits the compromised page. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, execute malicious code, and use the victim's identity to take actions on the site on behalf of the user, such as change permissions and delete content. The security update addresses the vulnerability by ensuring that Team Foundation Server sanitizes user inputs. **FAQ:** None **Mitigations:**	Low	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0777						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Team Foundation Server 2018 Updated 1.2	Release Notes Security Update	Low	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0777						
Team Foundation Server 2017 Update 3.1	Release Notes Security Update	Low	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Unknown
Team Foundation Server 2018 Update 3.2	Release Notes Security Update	Low	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0778 - Microsoft Office SharePoint XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0778 MITRE NVD	**CVE Title:** Microsoft Office SharePoint XSS Vulnerability **Description:** A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's	Important	Tampering

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0778						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2013 Service Pack 1	4462208 Security Update	Important	Tampering	4462143	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4462211 Security Update	Important	Tampering	4462155	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0779 - Microsoft Edge Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0779 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	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge, and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements by adding specially crafted content that could exploit the vulnerability. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by way of enticement in an email or Instant Messenger message, or by getting them to open an attachment sent through email. The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0779						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows Server 2016	4489882 Security Update	Low	Information Disclosure	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4489882 Security	Important	Information Disclosure	4487026	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0779						
Windows 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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0779						
1703 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 ARM64-	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0779						
based Systems						

CVE-2019-0780 - Microsoft Browser Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0780 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.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0780						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Important	Remote Code Execution	4486474	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	4489878 Monthly Rollup 4489873 IE Cumulative	Important	Remote Code Execution	4486474	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-2019-0780						
Service Pack 1						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Low	Remote Code Execution	4486474	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	4489873 IE Cumulative 4489881 Monthly Rollup	Important	Remote Code Execution	4487000	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	4489873 IE Cumulative 4489881	Important	Remote Code Execution	4487000	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0780						
Windows 8.1 for x64-based systems	Monthly Rollup				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 2012 R2	4489873 IE Cumulative 4489881 Monthly Rollup	Low	Remote Code Execution	4487000	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	4489881 Monthly Rollup	Important	Remote Code Execution	4487000	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	4489872 Security Update	Important	Remote Code Execution	4487018	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-2019-0780						
Internet Explorer 11 on Windows 10 for x64-based Systems	4489872 Security Update	Important	Remote Code Execution	4487018	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	4489882 Security Update	Low	Remote Code Execution	4487026	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	4489882 Security Update	Important	Remote Code Execution	4487026	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-2019-0780						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Remote Code Execution	4487026	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	4489871 Security Update	Important	Remote Code Execution	4487020	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	4489871 Security Update	Important	Remote Code Execution	4487020	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-2019-0780						
x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	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	4489868 Security Update	Important	Remote Code Execution	4487017	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-2019-0780						
1803 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	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 1803 for ARM64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	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	4489899 Security	Important	Remote Code Execution	4487044	Base: 7.5 Temporal: 6.7	Yes

CVE-2019-0780						
Windows 10 Version 1809 for 32-bit Systems	Update				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 1809 for x64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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 1809 for ARM64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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-2019-0780						
Internet Explorer 11 on Windows Server 2019	4489899 Security Update	Low	Remote Code Execution	4487044	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 1709 for ARM64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 10 on Windows Server 2012	4489873 IE Cumulative 4489891 Monthly Rollup	Low	Remote Code Execution	4487025	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-2019-0780						
Microsoft Edge on Windows 10 for 32-bit Systems	4489872 Security Update	Important	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489872 Security Update	Important	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Low	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489882 Security Update	Important	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0780						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489871 Security Update	Important	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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	4489871 Security Update	Important	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0780						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for 32-bit Systems	4489868 Security Update	Important	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0780						
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1803 for ARM64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for 32-bit Systems	4489899 Security Update	Important	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0780						
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 1809 for ARM64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC: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 2019	4489899 Security Update	Low	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4489886 Security	Important	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0780						
10 Version 1709 for ARM64-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	

CVE-2019-0782 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0782 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.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: **What type of information could be disclosed by this vulnerability?** The type of information that could be disclosed if an attacker successfully exploited this vulnerability is uninitialized memory and kernel memory - unintentional read access to memory contents in kernel space from a user mode process. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0782						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0782						
(Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489880 Monthly Rollup 4489876 Security	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0782						
(Server Core installation)	Only					
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0782						
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489881 Monthly Rollup 4489883 Security	Important	Information Disclosure	4487000	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0782						
	Only					
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489872 Security Update	Important	Information Disclosure	4487018	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0782						
Windows Server 2016 (Server Core installation)	4489882 Security Update	Important	Information Disclosure	4487026	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489871 Security Update	Important	Information Disclosure	4487020	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0782						
Windows Server, version 1709 (Server Core Installation)	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 for 32-bit Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 for x64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1803 (Server Core Installation)	4489868 Security Update	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489868 Security	Important	Information Disclosure	4487017	Base: 4.7 Temporal: 4.2	Yes

CVE-2019-0782						
1803 for ARM64-based Systems	Update				Vector: CVSS: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 1809 for 32-bit Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1809 for x64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 1809 for ARM64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 2019	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0782						
Windows Server 2019 (Server Core installation)	4489899 Security Update	Important	Information Disclosure	4487044	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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 ARM64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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	4489880 Monthly Rollup 4489876 Security	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0782						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/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)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0783 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0783 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 Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.	Important	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 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0783						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489873 IE Cumulative	Important	Remote Code Execution	4486474	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	4489878 Monthly Rollup 4489873 IE Cumulative	Important	Remote Code Execution	4486474	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	4489878 Monthly Rollup	Low	Remote Code Execution	4486474	Base: 6.4 Temporal: 5.8	Yes

CVE-2019-0783						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489873 IE Cumulative				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	
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4489873 IE Cumulative 4489881 Monthly Rollup	Important	Remote Code Execution	4487000	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	4489873 IE Cumulative 4489881 Monthly Rollup	Important	Remote Code Execution	4487000	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-2019-0783						
Internet Explorer 11 on Windows Server 2012 R2	4489873 IE Cumulative 4489881 Monthly Rollup	Low	Remote Code Execution	4487000	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	4489881 Monthly Rollup	Important	Remote Code Execution	4487000	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	4489872 Security Update	Important	Remote Code Execution	4487018	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	4489872 Security Update	Important	Remote Code Execution	4487018	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-2019-0783						
x64-based Systems						
Internet Explorer 11 on Windows Server 2016	4489882 Security Update	Low	Remote Code Execution	4487026	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	4489882 Security Update	Important	Remote Code Execution	4487026	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	4489882 Security Update	Important	Remote Code Execution	4487026	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-2019-0783						
1607 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Remote Code Execution	4487020	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	4489871 Security Update	Important	Remote Code Execution	4487020	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-2019-0783						
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Remote Code Execution	4486996	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	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	4489868 Security Update	Important	Remote Code Execution	4487017	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-2019-0783						
Version 1803 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	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 1803 for ARM64-based Systems	4489868 Security Update	Important	Remote Code Execution	4487017	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-2019-0783						
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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 1809 for x64-based Systems	4489899 Security Update	Important	Remote Code Execution	4487044	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	4489899 Security Update	Important	Remote Code Execution	4487044	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-2019-0783						
Version 1809 for ARM64-based Systems						
Internet Explorer 11 on Windows Server 2019	4489899 Security Update	Low	Remote Code Execution	4487044	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 1709 for ARM64-based Systems	4489886 Security Update	Important	Remote Code Execution	4486996	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-2019-0783						
Internet Explorer 10 on Windows Server 2012	4489873 IE Cumulative 4489891 Monthly Rollup	Low	Remote Code Execution	4487025	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-2019-0784 - Windows ActiveX Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0784 MITRE NVD	**CVE Title:** Windows ActiveX Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that the ActiveX Data objects (ADO) handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	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 Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the ActiveX Data objects handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0784						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Critical	Remote Code Execution	4486563	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Critical	Remote Code Execution	4486563	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0784						
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4489878 Monthly Rollup 4489885 Security Only	Critical	Remote Code Execution	4486563	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Critical	Remote Code Execution	4486563	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Critical	Remote Code Execution	4486563	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0784						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Critical	Remote Code Execution	4487019	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Critical	Remote Code Execution	4487025	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Critical	Remote Code Execution	4487025	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0784						
Windows 8.1 for 32-bit systems	4489881 Monthly Rollup 4489883 Security Only	Critical	Remote Code Execution	4487000	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security Only	Critical	Remote Code Execution	4487000	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Critical	Remote Code Execution	4487000	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0784						
Windows RT 8.1	4489881 Monthly Rollup	Critical	Remote Code Execution	4487000	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4489881 Monthly Rollup 4489883 Security Only	Critical	Remote Code Execution	4487000	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Unknown
Windows 10 for 32-bit Systems	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4489872 Security Update	Critical	Remote Code Execution	4487018	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0784						
Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4489882 Security Update	Critical	Remote Code Execution	4487026	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Critical	Remote Code Execution	4487020	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709	4489886 Security	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8	Yes

CVE-2019-0784						
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	
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0784						
(Server Core Installation)						
Windows 10 Version 1803 for ARM64-based Systems	4489868 Security Update	Critical	Remote Code Execution	4487017	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0784						
Windows Server 2019 (Server Core installation)	4489899 Security Update	Critical	Remote Code Execution	4487044	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Critical	Remote Code Execution	4486996	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Critical	Remote Code Execution	4487019	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Critical	Remote Code Execution	4487019	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0784						
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Critical	Remote Code Execution	4487019	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Critical	Remote Code Execution	4487019	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0797 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0797 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how Win32k handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0797						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Important	Elevation of Privilege	4487025	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-2019-0797						
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Important	Elevation of Privilege	4487025	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	4489881 Monthly Rollup 4489883 Security Only	Important	Elevation of Privilege	4487000	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	Unknown
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security Only	Important	Elevation of Privilege	4487000	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	Unknown

CVE-2019-0797						
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Elevation of Privilege	4487000	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	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Elevation of Privilege	4487000	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)	4489881 Monthly Rollup 4489883 Security Only	Important	Elevation of Privilege	4487000	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	Unknown
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Elevation of Privilege	4487018	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-2019-0797						
Windows 10 for x64-based Systems	4489872 Security Update	Important	Elevation of Privilege	4487018	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	4489882 Security Update	Important	Elevation of Privilege	4487026	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Important	Elevation of Privilege	4487026	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	4489882 Security Update	Important	Elevation of Privilege	4487026	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)	4489882 Security Update	Important	Elevation of Privilege	4487026	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	4489871 Security	Important	Elevation of Privilege	4487020	Base: 7 Temporal: 6.3	Yes

CVE-2019-0797						
for 32-bit Systems	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 1703 for x64-based Systems	4489871 Security Update	Important	Elevation of Privilege	4487020	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	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)	4489886 Security Update	Important	Elevation of Privilege	4486996	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 1803 for 32-bit Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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-2019-0797						
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 (Server Core Installation)	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1803 for ARM64-based Systems	4489868 Security Update	Important	Elevation of Privilege	4487017	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 1809 for 32-bit Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 1809 for x64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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-2019-0797						
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Elevation of Privilege	4487044	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 2019	4489899 Security Update	Important	Elevation of Privilege	4487044	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 2019 (Server Core installation)	4489899 Security Update	Important	Elevation of Privilege	4487044	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Elevation of Privilege	4486996	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-2019-0798 - Skype for Business and Lync Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0798 MITRE NVD	**CVE Title:** Skype for Business and Lync Spoofing Vulnerability **Description:** A spoofing vulnerability exists when a Lync Server or Skype for Business Server does not properly sanitize a specially crafted request. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected server. The attacker who successfully exploited this vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. For the vulnerability to be exploited, a user must click a specially crafted URL that takes the user to a targeted Lync or Skype for Business site. In an email attack scenario, an attacker could exploit the vulnerability by sending an email message containing the specially crafted URL to the user of the targeted Lync or Skype for Business site and convincing the user to click the specially crafted URL. The security update addresses the vulnerability by helping to ensure that Lync Server and Skype for Business Server properly sanitize web requests. **FAQ:**	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0798						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0798						
Skype for Business Server 2015 March 2019 Update	3061064 Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Lync Server 2013 July 2018 Update	2809243 Security Update	Important	Spoofing		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0808 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0808 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Win32k component 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 that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how Win32k handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0808						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Elevation of Privilege	4486563	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	4489878 Monthly Rollup 4489885 Security Only	Important	Elevation of Privilege	4486563	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	4489878 Monthly Rollup 4489885 Security Only	Important	Elevation of Privilege	4486563	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-2019-0808						
Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Elevation of Privilege	4486563	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	4489878 Monthly Rollup 4489885 Security Only	Important	Elevation of Privilege	4486563	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	4489880 Monthly Rollup 4489876 Security	Important	Elevation of Privilege	4487019	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-2019-0808						
Core installation)	Only					
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Elevation of Privilege	4487019	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	4489880 Monthly Rollup 4489876 Security Only	Important	Elevation of Privilege	4487019	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	4489880 Monthly Rollup 4489876 Security Only	Important	Elevation of Privilege	4487019	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-2019-0808						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Elevation of Privilege	4487019	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-2019-0809 - Visual Studio Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0809 MITRE NVD	**CVE Title:** Visual Studio Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when the Visual Studio C++ Redistributable Installer improperly validates input before loading dynamic link library (DLL) files. An attacker who successfully exploited the vulnerability could execute arbitrary code in the context of the current user. 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
	To exploit the vulnerability, an attacker must place a malicious DLL on a local system and convince a user to execute a specific executable. The security update addresses the vulnerability by correcting how the Visual Studio C++ Redistributable Installer validates input before loading DLL files. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0809						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Visual Studio 2017 version 15.9	Release Notes Security Update	Important	Remote Code Execution		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2019-0816 - Azure SSH Keypairs Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0816 MITRE NVD	**CVE Title:** Azure SSH Keypairs Security Feature Bypass Vulnerability **Description:** A security feature bypass exists in Azure SSH Keypairs, due to a change in the provisioning logic for some Linux images that use cloud-init. Extraneous Microsoft service public keys can be unexpectedly added to the VM authorized keys file in the limited scenarios described in 4491476.Â For more information on how to know if you are affected and how to protect yourself, please see 4491476. This update addresses this vulnerability by preventing these keys from being added.	Moderate	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0816						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2019-0816						
UbuntuServer:18.04-LTS	4491476 Security Update	Moderate	Security Feature Bypass		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2019-0821 - Windows SMB Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2019-0821 MITRE NVD	**CVE Title:** Windows SMB Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests. An authenticated attacker who successfully exploited this vulnerability could craft a special packet, which could lead to information disclosure from the server. To exploit the vulnerability, an attacker would have to be able to authenticate and send SMB messages to an impacted Windows SMB Server The security update addresses the vulnerability by correcting how Windows SMB Server handles authenticated requests. **FAQ:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	What type of information could be disclosed by this vulnerability? The type of information that could be disclosed if an attacker successfully exploited this vulnerability is memory layout - the vulnerability allows an attacker to collect information that facilitates predicting addressing of the memory. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/12/2019 07:00:00 Information published.		

Affected Software

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

CVE-2019-0821						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0821						
(Server Core installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4489878 Monthly Rollup 4489885 Security Only	Important	Information Disclosure	4486563	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0821						
(Server Core installation)	Only					
Windows Server 2012	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4489884 Security Only 4489891 Monthly Rollup	Important	Information Disclosure	4487025	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0821						
Windows 8.1 for x64-based systems	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows Server 2012 R2	4489881 Monthly Rollup 4489883 Security Only	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown
Windows RT 8.1	4489881 Monthly Rollup	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4489881 Monthly Rollup 4489883 Security	Important	Information Disclosure	4487000	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Unknown

CVE-2019-0821						
	Only					
Windows 10 for 32-bit Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4489872 Security Update	Important	Information Disclosure	4487018	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4489882 Security Update	Important	Information Disclosure	4487026	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4489882 Security Update	Important	Information Disclosure	4487026	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4489882 Security Update	Important	Information Disclosure	4487026	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0821						
Windows Server 2016 (Server Core installation)	4489882 Security Update	Important	Information Disclosure	4487026	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4489871 Security Update	Important	Information Disclosure	4487020	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4489871 Security Update	Important	Information Disclosure	4487020	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0821						
Windows Server, version 1709 (Server Core Installation)	4489886 Security Update	Important	Information Disclosure	4486996	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for 32-bit Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1803 for x64-based Systems	4489868 Security Update	Important	Information Disclosure	4487017	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1803 (Server Core Installation)	4489868 Security Update	Important	Information Disclosure	4487017	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version	4489868 Security	Important	Information Disclosure	4487017	Base: 6.5 Temporal: 5.9	Yes

CVE-2019-0821						
1803 for ARM64-based Systems	Update				Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1809 for 32-bit Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for x64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1809 for ARM64-based Systems	4489899 Security Update	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2019	4489899 Security Update	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0821						
Windows Server 2019 (Server Core installation)	4489899 Security Update	Important	Information Disclosure	4487044	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for ARM64-based Systems	4489886 Security Update	Important	Information Disclosure	4486996	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2019-0821						
	Only					
Windows Server 2008 for x64-based Systems Service Pack 2	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4489880 Monthly Rollup 4489876 Security Only	Important	Information Disclosure	4487019	Base: 6.5 Temporal: 5.9 Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

Statement

==========

About NSFOCUS

==========

NSFOCUS IB is a wholly owned subsidiary of NSFOCUS, an enterprise application and network security provider, with operations in the Americas, Europe, the Middle East, Southeast Asia and Japan. NSFOCUS IB has a proven track record of combatting the increasingly complex cyber threat landscape through the construction and implementation of multi-layered defense systems. The company's Intelligent Hybrid Security strategy utilizes both cloud and on-premises security platforms, built on a foundation of real-time global threat intelligence, to provide unified, multi-layer protection from advanced cyber threats.

For more information about NSFOCUS, please visit:

https://www.nsfocusglobal.com.

QR code of NSFOCUS at Sina Weibo

QR code of NSFOCUS at WeChat