ADV180006 - March 2018 Adobe Flash Security Update

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV180006 MITRE NVD	**CVE Title:** March 2018 Adobe Flash Security Update **Description:** This security update addresses the following vulnerabilities, which are described in Adobe Security Bulletin APSB18-05: CVE-2018-4919 and CVE-2018-4920. **FAQ:** **How could an attacker exploit these vulnerabilities?** In a web-based attack scenario where the user is using Internet Explorer for the desktop, an attacker could host a specially crafted website that is designed to exploit any of these vulnerabilities through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an	Critical	Remote Code Execution

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

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	7. "Compatibility Flags"=dword:00000400 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.		

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1. Create a text file named Disable_Flash.reg with the following contents: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Common\COM\Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] "Compatibility Flags"=dword:00000400 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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	ActiveX controls may not display as intended. **How to undo the workaround**. To re-enable ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, perform the following steps: 1. Click File, click Options, click Trust Center, and then click Trust Center Settings. 2. Click ActiveX Settings in the left-hand pane, and then deselect Disable all controls without notifications. 3. Click OK to save your settings. **Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones** You can help protect against exploitation of these vulnerabilities by changing your settings for the Internet security zone to block ActiveX controls and Active Scripting. You can do this by setting your browser security to High. To raise the browsing security level in Internet Explorer, perform the following steps: 1. On the Internet Explorer **Tools** menu, click** Internet Option**s. 2. In the **Internet Options** dialog box, click the **Security** tab, and then click **Internet**. 3. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	4. Click **Local intranet**. 5. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 6. Click **OK** to accept the changes and return to Internet Explorer. **Note** If no slider is visible, click **Default Level**, and then move the slider to **High**. **Note** Setting the level to High may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly even with the security setting set to High. **Impact of workaround**. There are side effects to blocking ActiveX Controls and Active Scripting. Many websites on the Internet or an intranet use ActiveX or Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX Controls to provide menus, ordering forms, or even account statements. Blocking ActiveX Controls or Active Scripting is a global setting that affects all Internet and intranet sites. If you do not want to block ActiveX Controls or Active Scripting for such sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". **Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone** You can help protect against exploitation of these vulnerabilities by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	zone. To do this, perform the following steps: 1. In Internet Explorer, click **Internet Options** on the **Tools** menu. 2. Click the **Security** tab. 3. Click **Internet**, and then click **Custom Level**. 4. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 5. Click **Local intranet**, and then click **Custom Level**. 6. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 7. Click **OK** to return to Internet Explorer, and then click **OK** again. **Note** Disabling Active Scripting in the Internet and Local intranet security zones may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly. **Impact of workaround**. There are side effects to prompting before running Active Scripting. Many websites that are on the Internet or on an intranet use Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use Active Scripting to provide menus, ordering forms, or even account statements. Prompting before running Active Scripting is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you feel you		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	trust the site that you are visiting, click **Yes** to run Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". **Add sites that you trust to the Internet Explorer Trusted sites zone** After you set Internet Explorer to require a prompt before it runs ActiveX controls and Active Scripting in the Internet zone and in the Local intranet zone, you can add sites that you trust to the Internet Explorer Trusted sites zone. This will allow you to continue to use trusted websites exactly as you do today, while helping to protect you from this attack on untrusted sites. We recommend that you add only sites that you trust to the Trusted sites zone. To do this, perform the following steps: 1. In Internet Explorer, click **Tools**, click **Internet Options**, and then click the **Security** tab. 2. In the **Select a web content zone to specify its current security settings** box, click **Trusted Sites**, and then click **Sites**. 3. If you want to add sites that do not require an encrypted channel, click to clear the **Require server verification (https:) for all sites in this zone** check box. 4. In the **Add this website to the zone** box, type the URL of a site that you trust, and then click **Add**. 5. Repeat these steps for each site that you want to add to the zone. 6. Click **OK** two times to accept the changes and return to Internet Explorer. **Note** Add any sites		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	that you trust not to take malicious action on your system. Two sites in particular that you may want to add are ***.windowsupdate.microsoft.com** and ***.update.microsoft.com**. These are the sites that will host the update, and they require an ActiveX control to install the update. **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

ADV180006						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Adobe Flash Player on Windows Server	4088785 Security	Critical	Remote Code	4056887	Base: N/A	Yes

ADV180006						
2012	Update		Execution		Temporal: N/A Vector: N/A	
Adobe Flash Player on Windows 8.1 for 32-bit systems	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for x64-based systems	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2012 R2	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows RT 8.1	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 for 32-bit Systems	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV180006						
Adobe Flash Player on Windows 10 for x64-based Systems	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1511 for x64-based Systems	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1511 for 32-bit Systems	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2016	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A	Yes

ADV180006						
					Vector: N/A	
Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for 32-bit Systems	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1709 for x64-based Systems	4088785 Security Update	Critical	Remote Code Execution	4056887	Base: N/A Temporal: N/A Vector: N/A	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0787 MITRE NVD	**CVE Title:** ASP.NET Core Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when a Kestrel web application fails to validate web requests. An attacker who successfully exploited this vulnerability could perform HTML injection attacks. To exploit the vulnerability, an attacker could send a specially crafted request, containing injected HTML, to the web application. The specially crafted request would initiate a "password reset" email to the target user. Depending on the target user email client, the injected HTML could trigger as soon as the target user opens the "password reset" e-mail. The security update addresses the vulnerability by correcting how a Kestrel web application validates web requests. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0787						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
ASP.NET Core 2.0	Commit Security Update	Important	Elevation of Privilege		Base: N/A Temporal: N/A Vector: N/A	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0808 MITRE NVD	**CVE Title:** ASP.NET Core Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when ASP.NET Core improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against an ASP.NET Core web application. The vulnerability can be exploited remotely, without authentication. A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the .NET Core application. The update addresses the vulnerability by correcting how the ASP.NET Core web application handles web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0808						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
ASP.NET Core 2.0	Commit Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-0811 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0811 MITRE 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:** None **Mitigations:** None **Workarounds:** None **Revision:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0811						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0811						
	Rollup					
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for	4088878 Security	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2018-0811						
Itanium-Based Systems Service Pack 1	Only 4088875 Monthly Rollup				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 Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4089344 Security Update	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows	408887	Importan	Informatio	4074593	Base: 5.5	Yes

CVE-2018-0811						
Server 2012	7 Monthly Rollup 4088880 Security Only	t	n Disclosure		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	
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879	Important	Information Disclosure	4074594	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0811						
	Security Only					
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4088876	Important	Information	4074594	Base: 5.5 Temporal: 5	Yes

CVE-2018-0811						
	Monthly Rollup		Disclosure		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 Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10	408877	Importan	Informatio	4074591	Base: 5.5	Yes

CVE-2018-0811						
Version 1511 for x64-based Systems	9 Security Update	t	n Disclosure		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	
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0811						
					C	
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709	4088776	Important	Information	4074588	Base: 5.5 Temporal: 5	Yes

CVE-2018-0811						
for x64-based Systems	Security Update		Disclosure		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 Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4089344 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4089344 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4089344 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0811						
Service Pack 2					C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4089344 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0813 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0813 MITRE 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	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	could obtain information to further compromise the userâ€™s system. The update addresses the vulnerability by correcting how the Windows kernel initializes objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0813						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008	4088878	Important	Information	4074598	Base: 5.5 Temporal: 5	Yes

CVE-2018-0813						
R2 for x64-based Systems Service Pack 1 (Server Core installation)	Security Only 4088875 Monthly Rollup		Disclosure		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 Server 2008 R2 for Itanium-Based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0813						
	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4089344 Security Update	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server 2012	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 408888	Important	Information Disclosure	4074593	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0813						
	0 Security Only					
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows	408887	Importan	Informatio	4074594	Base: 5.5	Yes

CVE-2018-0813						
Server 2012 R2	6 Monthly Rollup 4088879 Security Only	t	n Disclosure		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	
Windows RT 8.1	4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10	408878	Importan	Informatio	4074596	Base: 5.5	Yes

CVE-2018-0813						
for 32-bit Systems	6 Security Update	t	n Disclosure		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	
Windows 10 for x64-based Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0813						
					C	
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703	4088782	Important	Information	4074592	Base: 5.5 Temporal: 5	Yes

CVE-2018-0813						
for x64-based Systems	Security Update		Disclosure		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 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server 2008 for Itanium-Based Systems	4089344 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

CVE-2018-0813						
Service Pack 2						
Windows Server 2008 for 32-bit Systems Service Pack 2	4089344 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4089344 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4089344 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

CVE-2018-0814 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0814 MITRE 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:** None **Mitigations:** None **Workarounds:** None **Revision:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0814						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0814						
	Rollup					
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for	4088878 Security	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector:	Yes

CVE-2018-0814						
Itanium-Based Systems Service Pack 1	Only 4088875 Monthly Rollup				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 Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4089344 Security Update	Important	Information Disclosure	4074598	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows	408887	Importan	Informatio	4074593	Base: 5.5	Yes

CVE-2018-0814						
Server 2012	7 Monthly Rollup 4088880 Security Only	t	n Disclosure		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	
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879	Important	Information Disclosure	4074594	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0814						
	Security Only					
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4088876	Important	Information	4074594	Base: 5.5 Temporal: 5	Yes

CVE-2018-0814						
	Monthly Rollup		Disclosure		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 Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10	408877	Importan	Informatio	4074591	Base: 5.5	Yes

CVE-2018-0814						
Version 1511 for x64-based Systems	9 Security Update	t	n Disclosure		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	
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0814						
					C	
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709	4088776	Important	Information	4074588	Base: 5.5 Temporal: 5	Yes

CVE-2018-0814						
for x64-based Systems	Security Update		Disclosure		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 Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4089344 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4089344 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes
Windows Server 2008 for x64-based Systems	4089344 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

CVE-2018-0814						
Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4089344 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0815 MITRE NVD	**CVE Title:** Windows GDI Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	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 the vulnerability by correcting how GDI handles objects in memory and by preventing instances of unintended user-mode privilege elevation. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0815						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008	4088878 Security	Important	Elevation of	4074598	Base: 7 Temporal: 6.3	Yes

CVE-2018-0815						
R2 for x64-based Systems Service Pack 1 (Server Core installation)	Only 4088875 Monthly Rollup		Privilege		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 2008 R2 for Itanium-Based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit	4089344 Security Update	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector:	Yes

CVE-2018-0815						
Systems Service Pack 2 (Server Core installation)					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 2008 for Itanium-Based Systems Service Pack 2	4089344 Security Update	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4089344 Security Update	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4089344 Security Update	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based	4089344 Security Update	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector:	Yes

CVE-2018-0815						
Systems Service Pack 2 (Server Core installation)					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	

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0816 MITRE NVD	**CVE Title:** Windows GDI Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how GDI handles objects in	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	memory and by preventing instances of unintended user-mode privilege elevation. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0816						
Product	**KB**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart**

CVE-2018-0816						
	Article					**Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0816						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4089344 Security Update	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4088877 Monthly	Important	Elevation of	4074593	Base: 7 Temporal: 6.3	Yes

CVE-2018-0816						
	Rollup 4088880 Security Only		Privilege		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 2012 (Server Core installation)	4088877 Monthly Rollup 4088880 Security Only	Important	Elevation of Privilege	4074593	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879 Security Only	Important	Elevation of Privilege	4074594	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879	Important	Elevation of Privilege	4074594	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0816						
	Security Only					
Windows Server 2012 R2	4088876 Monthly Rollup 4088879 Security Only	Important	Elevation of Privilege	4074594	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4088876 Monthly Rollup	Important	Elevation of Privilege	4074594	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Elevation of Privilege	4074594	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit	4088786 Security	Important	Elevation of	4074596	Base: 7 Temporal: 6.3	Yes

CVE-2018-0816						
Systems	Update		Privilege		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 for x64-based Systems	4088786 Security Update	Important	Elevation of Privilege	4074596	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Elevation of Privilege	4074591	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Elevation of Privilege	4074591	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0816						
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4089344 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4089344 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0816						
Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2	4089344 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4089344 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0817 MITRE	**CVE Title:** Windows GDI Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
NVD	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses the vulnerability by correcting how GDI handles objects in memory and by preventing instances of unintended user-mode privilege elevation. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

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

CVE-2018-0817						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0817						
	Monthly Rollup					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems	4088878 Security Only 4088875 Monthly	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0817						
Service Pack 1	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4089344 Security Update	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4088877 Monthly Rollup 4088880 Security Only	Important	Elevation of Privilege	4074593	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880 Security Only	Important	Elevation of Privilege	4074593	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0817						
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879 Security Only	Important	Elevation of Privilege	4074594	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Elevation of Privilege	4074594	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4088876 Monthly Rollup 4088879 Security Only	Important	Elevation of Privilege	4074594	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4088876 Monthly	Important	Elevation of	4074594	Base: 7 Temporal: 6.3	Yes

CVE-2018-0817						
	Rollup		Privilege		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 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Elevation of Privilege	4074594	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Elevation of Privilege	4074596	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Elevation of Privilege	4074596	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Elevation of Privilege	4074591	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511	4088779 Security	Important	Elevation of	4074591	Base: 7 Temporal: 6.3	Yes

CVE-2018-0817						
for 32-bit Systems	Update		Privilege		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 2016	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0817						
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4089344 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0817						
Windows Server 2008 for 32-bit Systems Service Pack 2	4089344 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4089344 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4089344 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0868 MITRE NVD	**CVE Title:** Windows Installer Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior. A locally authenticated attacker could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by correcting the input sanitization error to preclude unintended elevation. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0868						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0868						
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Base	4088878 Security Only	Important	Elevation of Privilege	4074598	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:	Yes

CVE-2018-0868						
d Systems Service Pack 1	4088875 Monthly Rollup				C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4087398 Security Update	Important	Elevation of Privilege	4074598	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4088877	Important	Elevation of	4074593	Base: 7.4 Temporal: 6.7	Yes

CVE-2018-0868						
	Monthly Rollup 4088880 Security Only		Privilege		Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880 Security Only	Important	Elevation of Privilege	4074593	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879 Security	Important	Elevation of Privilege	4074594	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0868						
	Only					
Windows Server 2012 R2	4088876 Monthly Rollup 4088879 Security Only	Important	Elevation of Privilege	4074594	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4088876 Monthly Rollup	Important	Elevation of Privilege	4074594	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security	Important	Elevation of Privilege	4074594	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0868						
	Only					
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Elevation of Privilege	4074596	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Elevation of Privilege	4074596	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Elevation of Privilege	4074591	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Elevation of Privilege	4074591	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows	408878	Importan	Elevatio	4074590	Base: 7.4	Yes

CVE-2018-0868						
Server 2016	7 Security Update	t	n of Privilege		Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:	Yes

CVE-2018-0868						
					C	
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008	4087398	Important	Elevation of	4074588	Base: 7.4 Temporal: 6.7	Yes

CVE-2018-0868						
for Itanium-Based Systems Service Pack 2	Security Update		Privilege		Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2	4087398 Security Update	Important	Elevation of Privilege	4074588	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4087398 Security Update	Important	Elevation of Privilege	4074588	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4087398 Security Update	Important	Elevation of Privilege	4074588	Base: 7.4 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0872 MITRE 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	exploit the vulnerability. The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0872						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4088786 Security Update	Critical	Remote Code Execution	4074596	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4088786 Security Update	Critical	Remote Code Execution	4074596	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2018-0872						
Version 1511 for 32-bit Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows Server 2016	4088787 Security Update	Moderate	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft	4088782	Critical	Remote	4074592	Base: 4.2	Yes

CVE-2018-0872						
Edge on Windows 10 Version 1703 for 32-bit Systems	Security Update		Code Execution		Temporal: 3.8 Vector: CVSS: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 x64-based Systems	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2018-0872						
Version 1709 for x64-based Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0873 MITRE 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	Important	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0873						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0873						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4088787 Security Update	Low	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for	4088787 Security Update	Important	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0873						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0873						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Only	Important	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0874 MITRE	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0874						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit	4088786 Security Update	Critical	Remote Code Execution	4074596	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0874						
Systems						
Microsoft Edge on Windows 10 for x64-based Systems	4088786 Security Update	Critical	Remote Code Execution	4074596	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4088787 Security	Moderate	Remote Code	4074590	Base: 4.2 Temporal: 3.8	Yes

CVE-2018-0874						
Windows Server 2016	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0874						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security	Critical	Remote Code	4074588	Base: 4.2 Temporal: 3.8	Yes

CVE-2018-0874						
	Only		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0875 MITRE NVD	**CVE Title:** .NET Core Denial of Service Vulnerability **Description:** A denial of service vulnerability exists in the way that .NET Core handles specially crafted requests, causing a hash collision. To exploit the vulnerability, an attacker could send a small number of specially crafted requests to an .NET Core web application, causing performance to degrade significantly enough to cause a denial of service condition. The security update addresses the vulnerability by correcting how .NET Core handles specially crafted requests to prevent a hash collision. **FAQ:** None	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0875						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
.NET Core 1.0	Commit Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Yes

CVE-2018-0875						
.NET Core 1.1	Commit Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Yes
.NET Core 2.0	Commit Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Yes
PowerShell Core 6.0.0	Release Notes Security Update	Important	Denial of Service		Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0876 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0876 MITRE 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	Critical	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0876						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4088786 Security Update	Critical	Remote Code Execution	4074596	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4088786 Security	Critical	Remote Code	4074596	Base: 4.2 Temporal: 3.8	Yes

CVE-2018-0876						
Windows 10 for x64-based Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4088787 Security Update	Moderate	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft	4088787	Critical	Remote	4074590	Base: 4.2	Yes

CVE-2018-0876						
Edge on Windows 10 Version 1607 for 32-bit Systems	Security Update		Code Execution		Temporal: 3.8 Vector: CVSS: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	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2018-0876						
10 Version 1703 for x64-based Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0877 MITRE NVD	**CVE Title:** Windows Desktop Bridge VFS Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Desktop Bridge VFS does not take into acccount user/kernel mode when managing file paths. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows Desktop Bridge VFS handles file path management. **FAQ:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0877						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2016	4088787 Security	Important	Elevation of	4074590	Base: 7 Temporal: 6.7	Yes

CVE-2018-0877						
	Update		Privilege		Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version	4088782 Security	Important	Elevation of	4074592	Base: 7 Temporal: 6.7	Yes

CVE-2018-0877						
1703 for x64-based Systems	Update		Privilege		Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0878 MITRE NVD	**CVE Title:** Windows Remote Assistance Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Windows Remote Assistance incorrectly processes XML External Entities (XXE). An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit this condition, an attacker would need to send a specially crafted Remote Assistance invitation file to a user. A attacker could then steal text files from known locations on the victim's machine, under the context of the user, or alternatively, steal text information from URLs accessible to the victim. The stolen information could be submitted as part of the URL in HTTP request(s) to the attacker. In all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. Note that the information disclosure vulnerability by itself would not be sufficient	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	for an attacker to compromise a system. However, an attacker could combine this vulnerability with additional vulnerabilities to further exploit the system. The update addresses the vulnerability by correcting how Windows Remote Assistance processes XML External Entities (XXE). **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0878						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0878						
(Server Core installation)						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4089453 Security Update	Important	Information Disclosure	4074598	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4088877 Monthly Rollup	Important	Information Disclosure	4074593	Base: 3.1 Temporal: 2.8 Vector:	Yes

CVE-2018-0878						
	4088880 Security Only				CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security	Important	Information Disclosure	4074594	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0878						
	Only					
Windows Server 2012 R2	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit	4088786 Security Update	Important	Information Disclosure	4074596	Base: 3.1 Temporal: 2.8 Vector:	Yes

CVE-2018-0878						
Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 for x64-based Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit	4088787 Security Update	Important	Information Disclosure	4074590	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0878						
Systems						
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Information Disclosure	4074590	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows	4088776	Important	Information	4074588	Base: 3.1	Yes

CVE-2018-0878						
10 Version 1709 for 32-bit Systems	Security Update		Disclosure		Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Information Disclosure	4074588	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4089453 Security Update	Important	Information Disclosure	4074588	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0878						
Windows Server 2008 for x64-based Systems Service Pack 2	4089453 Security Update	Important	Information Disclosure	4074588	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4089453 Security Update	Important	Information Disclosure	4074588	Base: 3.1 Temporal: 2.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0879 - Microsoft Edge Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0879 MITRE NVD	**CVE Title:** Microsoft Edge Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory. **FAQ:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0879						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on	4088776 Security	Important	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9	Yes

CVE-2018-0879						
Windows 10 Version 1709 for 32-bit 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	
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0880 MITRE NVD	**CVE Title:** Windows Desktop Bridge Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when Desktop Bridge does	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	not properly manage the virtual registry. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows Desktop Bridge manages the virtual registry. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0880						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2016	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security	Important	Elevation of	4074590	Base: 7 Temporal: 6.7	Yes

CVE-2018-0880						
(Server Core installation)	Update		Privilege		Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows	4088776	Important	Elevation	4074588	Base: 7	Yes

CVE-2018-0880						
Server, version 1709 (Server Core Installation)	Security Update		of Privilege		Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0881 MITRE NVD	**CVE Title:** Microsoft Video Control Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Microsoft Video Control mishandles objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in system mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Microsoft Video Control handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0881						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes

CVE-2018-0881						
installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Elevation of Privilege	4074598	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2012	4088877 Monthly Rollup 4088880 Security Only	Important	Elevation of Privilege	4074593	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows	4088877	Important	Elevation	4074593	Base: 7	Yes

CVE-2018-0881						
Server 2012 (Server Core installation)	Monthly Rollup 4088880 Security Only		of Privilege		Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879 Security Only	Important	Elevation of Privilege	4074594	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Elevation of Privilege	4074594	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2012 R2	4088876 Monthly Rollup	Important	Elevation of Privilege	4074594	Base: 7 Temporal: 6.7 Vector:	Yes

CVE-2018-0881						
	4088879 Security Only				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	
Windows RT 8.1	4088876 Monthly Rollup	Important	Elevation of Privilege	4074594	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Elevation of Privilege	4074594	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Elevation of Privilege	4074596	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Elevation of Privilege	4074596	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes

CVE-2018-0881						
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Elevation of Privilege	4074591	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Elevation of Privilege	4074591	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2016 (Server Core	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.7 Vector:	Yes

CVE-2018-0881						
installation)					CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0882 MITRE NVD	**CVE Title:** Windows Desktop Bridge Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when Desktop Bridge does not properly manage the virtual registry. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows Desktop Bridge manages the virtual registry. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0882						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2016	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.7 Vector:	Yes

CVE-2018-0882						
					CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O	
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 7 Temporal: 6.7 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0883 MITRE NVD	**CVE Title:** Windows Shell Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Windows Shell does not properly validate file copy destinations. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. To exploit the vulnerability, a user must open a specially crafted file. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and then convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file designed to exploit the vulnerability. An attacker would have	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	no way to force a user to visit the website. Instead, an attacker would have to convince a user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file. The security update addresses the vulnerability by helping to ensure that Windows Shell validates file copy destinations. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0883						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Remote Code Execution	4074598	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Remote Code Execution	4074598	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008	4088878 Security	Important	Remote Code	4074598	Base: 5 Temporal: 4.5	Yes

CVE-2018-0883						
R2 for x64-based Systems Service Pack 1 (Server Core installation)	Only 4088875 Monthly Rollup		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Remote Code Execution	4074598	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Remote Code Execution	4074598	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit	4089175 Security Update	Important	Remote Code Execution	4074598	Base: 5 Temporal: 4.5 Vector:	Yes

CVE-2018-0883						
Systems Service Pack 2 (Server Core installation)					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	
Windows Server 2012	4088877 Monthly Rollup 4088880 Security Only	Important	Remote Code Execution	4074593	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880 Security Only	Important	Remote Code Execution	4074593	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879 Security	Important	Remote Code Execution	4074594	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2018-0883						
	Only					
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Remote Code Execution	4074594	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4088876 Monthly Rollup 4088879 Security Only	Important	Remote Code Execution	4074594	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4088876 Monthly Rollup	Important	Remote Code Execution	4074594	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server	4088876 Monthly Rollup	Important	Remote Code Execution	4074594	Base: 5 Temporal: 4.5 Vector:	Yes

CVE-2018-0883						
Core installation)	4088879 Security Only				CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Remote Code Execution	4074596	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Remote Code Execution	4074596	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Remote Code Execution	4074591	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Remote Code Execution	4074591	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Remote Code Execution	4074590	Base: 5 Temporal: 4.5 Vector:	Yes

CVE-2018-0883						
					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Remote Code Execution	4074590	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Remote Code Execution	4074590	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Remote Code Execution	4074590	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Remote Code Execution	4074592	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Remote Code Execution	4074592	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10	4088776	Important	Remote	4074588	Base: 5	Yes

CVE-2018-0883						
Version 1709 for 32-bit Systems	Security Update		Code Execution		Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Remote Code Execution	4074588	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4089175 Security Update	Important	Remote Code Execution	4074588	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4089175 Security Update	Important	Remote Code Execution	4074588	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4089175 Security Update	Important	Remote Code Execution	4074588	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2018-0883						
Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4089175 Security Update	Important	Remote Code Execution	4074588	Base: 5 Temporal: 4.5 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2018-0884 - Windows Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0884 MITRE NVD	**CVE Title:** Windows Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Windows Scripting Host which could allow an attacker to bypass Device Guard. An attacker who successfully exploited this vulnerability could circumvent a User Mode Code Integrity (UMCI) policy on the machine. To exploit the vulnerability, an attacker would first have to access the local	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	machine, and then run a malicious program. The update addresses the vulnerability by correcting how Windows Scripting Host handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0884						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Security Feature Bypass	4074596	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Security Feature Bypass	4074596	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Security Feature Bypass	4074591	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Security Feature Bypass	4074591	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Security Feature Bypass	4074590	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2018-0884						
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Security Feature Bypass	4074590	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Security Feature Bypass	4074590	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Security Feature Bypass	4074590	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Security Feature Bypass	4074592	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Security Feature Bypass	4074592	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit	4088776 Security Update	Important	Security Feature Bypass	4074588	Base: 5.3 Temporal: 4.8 Vector:	Yes

CVE-2018-0884						
Systems					CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Security Feature Bypass	4074588	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Security Feature Bypass	4074588	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0885 MITRE NVD	**CVE Title:** Windows Hyper-V Denial of Service Vulnerability **Description:** A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. An attacker who successfully exploited the vulnerability could	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	cause the host server to crash. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application that causes a host machine to crash. The update addresses the vulnerability by modifying how virtual machines access the Hyper-V Network Switch. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0885						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4088878 Security Only 4088875 Monthly Rollup	Important	Denial of Service	4074598	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Denial of Service	4074598	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0885						
Windows Server 2012	4088877 Monthly Rollup 4088880 Security Only	Important	Denial of Service	4074593	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880 Security Only	Important	Denial of Service	4074593	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Denial of Service	4074594	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4088876 Monthly	Important	Denial of	4074594	Base: 5.8 Temporal: 5.2	Yes

CVE-2018-0885						
R2	Rollup 4088879 Security Only		Service		Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows RT 8.1	4088876 Monthly Rollup	Important	Denial of Service	4074594	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Denial of Service	4074594	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Denial of Service	4074596	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for	4088779 Security Update	Important	Denial of Service	4074591	Base: 5.8 Temporal: 5.2 Vector:	Yes

CVE-2018-0885						
x64-based Systems					CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server 2016	4088787 Security Update	Important	Denial of Service	4074590	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Denial of Service	4074590	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Denial of Service	4074590	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Denial of Service	4074592	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for	4088776 Security Update	Important	Denial of Service	4074588	Base: 5.8 Temporal: 5.2 Vector:	Yes

CVE-2018-0885						
x64-based Systems					CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Denial of Service	4074588	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4073011 Security Update	Important	Denial of Service	4074588	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4073011 Security Update	Important	Denial of Service	4074588	Base: 5.8 Temporal: 5.2 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0886 - CredSSP Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0886 MITRE NVD	**CVE Title:** CredSSP Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the Credential Security Support Provider protocol (CredSSP). An attacker who successfully exploited this vulnerability could relay user credentials and use them to execute code on the target system. CredSSP is an authentication provider which processes authentication requests for other applications; any application which depends on CredSSP for authentication may be vulnerable to this type of attack. As an example of how an attacker would exploit this vulnerability against Remote Desktop Protocol, the attacker would need to run a specially crafted application and perform a man-in-the-middle attack against a Remote Desktop Protocol session. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by correcting how Credential Security Support Provider protocol (CredSSP) validates requests during the	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	authentication process. To be fully protected against this vulnerability users must enable Group Policy settings on their systems and update their Remote Desktop clients. The Group Policy settings are disabled by default to prevent connectivity problems and users must follow the instructions documented HERE to be fully protected. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0886						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Remote Code Execution	4074598	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875	Important	Remote Code Execution	4074598	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0886						
	Monthly Rollup					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4088878 Security Only 4088875 Monthly Rollup	Important	Remote Code Execution	4074598	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Remote Code Execution	4074598	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008	4088878	Important	Remote Code	4074598	Base: 7.1 Temporal: 6.4	Yes

CVE-2018-0886						
R2 for x64-based Systems Service Pack 1	Security Only 4088875 Monthly Rollup		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4056564 Security Update	Important	Remote Code Execution	4074598	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4088877 Monthly Rollup 4088880 Security Only	Important	Remote Code Execution	4074593	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0886						
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880 Security Only	Important	Remote Code Execution	4074593	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879 Security Only	Important	Remote Code Execution	4074594	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 408887	Important	Remote Code Execution	4074594	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0886						
	9 Security Only					
Windows Server 2012 R2	4088876 Monthly Rollup 4088879 Security Only	Important	Remote Code Execution	4074594	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4088876 Monthly Rollup	Important	Remote Code Execution	4074594	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 408887	Important	Remote Code Execution	4074594	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0886						
	9 Security Only					
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Remote Code Execution	4074596	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Remote Code Execution	4074596	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Remote Code Execution	4074591	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Remote Code Execution	4074591	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:	Yes

CVE-2018-0886						
					C	
Windows Server 2016	4088787 Security Update	Important	Remote Code Execution	4074590	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Remote Code Execution	4074590	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Remote Code Execution	4074590	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Remote Code Execution	4074590	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703	4088782	Important	Remote Code	4074592	Base: 7.1 Temporal: 6.4	Yes

CVE-2018-0886						
for 32-bit Systems	Security Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Remote Code Execution	4074592	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Remote Code Execution	4074588	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Remote Code Execution	4074588	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Remote Code Execution	4074588	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0886						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4056564 Security Update	Important	Remote Code Execution	4074588	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4056564 Security Update	Important	Remote Code Execution	4074588	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4056564 Security Update	Important	Remote Code Execution	4074588	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4056564 Security Update	Important	Remote Code Execution	4074588	Base: 7.1 Temporal: 6.4 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0888 MITRE NVD	**CVE Title:** Hyper-V Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. To exploit the vulnerability, an attacker on a guest operating system could run a specially crafted application that could cause the Hyper-V host operating system to disclose memory information. An attacker who successfully exploited the vulnerability could gain access to information on the Hyper-V host operating system. The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input. **FAQ:** None **Mitigations:** None **Workarounds:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0888						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 408887	Important	Information Disclosure	4074598	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0888						
	5 Monthly Rollup					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows	408887	Importan	Informatio	4074598	Base: 7.2	Yes

CVE-2018-0888						
Server 2008 R2 for x64-based Systems Service Pack 1	8 Security Only 4088875 Monthly Rollup	t	n Disclosure		Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	
Windows Server 2012	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880	Important	Information Disclosure	4074593	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0888						
	Security Only					
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4088876	Important	Information	4074594	Base: 7.2 Temporal: 6.5	Yes

CVE-2018-0888						
R2 (Server Core installation)	Monthly Rollup 4088879 Security Only		Disclosure		Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	
Windows 10 for x64-based Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10	408878	Importan	Informatio	4074590	Base: 7.2	Yes

CVE-2018-0888						
Version 1607 for x64-based Systems	7 Security Update	t	n Disclosure		Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Information Disclosure	4074590	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core	4088776 Security Update	Important	Information Disclosure	4074588	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0888						
Installation)					C	
Windows Server 2008 for x64-based Systems Service Pack 2	4088827 Security Update	Important	Information Disclosure	4074588	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4088827 Security Update	Important	Information Disclosure	4074588	Base: 7.2 Temporal: 6.5 Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0889 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0889 MITRE	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Moderate	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0889						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9	4089187 IE Cumulative	Moderate	Remote Code	4074736	Base: 6.4 Temporal: 5.8	Yes

CVE-2018-0889						
on Windows Server 2008 for 32-bit Systems Service Pack 2			Execution		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 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4089187 IE Cumulative	Moderate	Remote Code Execution	4074736	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for	4088875 Monthly Rollup 4089187 IE Cumulative	Critical	Remote Code Execution	4074736	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0889						
32-bit Systems Service Pack 1						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4088875 Monthly Rollup 4089187 IE Cumulative	Critical	Remote Code Execution	4074736	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service	4088875 Monthly Rollup 4089187 IE Cumulative	Moderate	Remote Code Execution	4074736	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0889						
Pack 1						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4089187 IE Cumulative 4088876 Monthly Rollup	Critical	Remote Code Execution	4074594	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4089187 IE Cumulative 4088876 Monthly Rollup	Critical	Remote Code Execution	4074594	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4089187 IE Cumulative 4088876 Monthly Rollup	Moderate	Remote Code Execution	4074594	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer	4088876 Monthly	Critical	Remote Code	4074594	Base: 7.5 Temporal: 6.7	Yes

CVE-2018-0889						
11 on Windows RT 8.1	Rollup		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 for 32-bit Systems	4088786 Security Update	Critical	Remote Code Execution	4074596	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4088786 Security Update	Critical	Remote Code Execution	4074596	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0889						
1511 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4088787 Security Update	Moderate	Remote Code Execution	4074590	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0889						
Version 1607 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet	4088782	Critical	Remote	4074592	Base: 7.5	Yes

CVE-2018-0889						
Explorer 11 on Windows 10 Version 1703 for x64-based Systems	Security Update		Code Execution		Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0889						
1709 for x64-based Systems						
Internet Explorer 10 on Windows Server 2012	4088877 Monthly Rollup 4089187 IE Cumulative	Moderate	Remote Code Execution	4074736	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0891 - Scripting Engine Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0891 MITRE NVD	**CVE Title:** Scripting Engine Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft browsers. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	In a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by changing how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0891						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4089187 IE Cumulative	Low	Information Disclosure	4074736	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server	4089187 IE Cumulative	Low	Information Disclosure	4074736	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0891						
2008 for x64-based Systems Service Pack 2						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4088875 Monthly Rollup 4089187 IE Cumulative	Important	Information Disclosure	4074736	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4088875 Monthly Rollup 4089187 IE Cumulative	Important	Information Disclosure	4074736	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet	4088875	Low	Informatio	4074736	Base: 6.4	Yes

CVE-2018-0891						
Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	Monthly Rollup 4089187 IE Cumulative		n Disclosure		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	
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4089187 IE Cumulative 4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based	4089187 IE Cumulative 4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0891						
systems						
Internet Explorer 11 on Windows Server 2012 R2	4089187 IE Cumulative 4088876 Monthly Rollup	Low	Information Disclosure	4074594	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4088786 Security Update	Important	Information Disclosure	4074596	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2018-0891						
Windows 10 for x64-based Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4088787 Security Update	Low	Information Disclosure	4074590	Base: 6.4 Temporal: 5.8 Vector:	Yes

CVE-2018-0891						
Windows Server 2016					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 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4088782 Security Update	Important	Information Disclosure	4074592	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:	Yes

CVE-2018-0891						
10 Version 1703 for 32-bit Systems					C	
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4088776 Security Update	Important	Information Disclosure	4074588	Base: 7.5 Temporal: 6.7 Vector:	Yes

CVE-2018-0891						
Windows 10 Version 1709 for x64-based Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 10 on Windows Server 2012	4088877 Monthly Rollup 4089187 IE Cumulative	Low	Information Disclosure	4074736	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for 32-bit Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0891						
Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4088787 Security Update	Low	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2018-0891						
10 Version 1607 for 32-bit Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0891						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Only	Important	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0893 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0893 MITRE 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0893						
Product	**KB**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart**

CVE-2018-0893						
	Article					**Required**
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4088787 Security Update	Moderate	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0893						
1607 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0893						
Systems						
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0894 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0894 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

Affected Software

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

CVE-2018-0894						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7	408887	Importan	Informatio	4074598	Base: 4.7	Yes

CVE-2018-0894						
for x64-based Systems Service Pack 1	8 Security Only 4088875 Monthly Rollup	t	n Disclosure		Temporal: 4.2 Vector: CVSS: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 (Server Core installation)	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4088878 Security Only 4088875	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0894						
	Monthly Rollup					
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4088877 Monthly Rollup	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0894						
	4088880 Security Only				C	
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0894						
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0894						
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0894						
					C	
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787	Important	Information	4074590	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0894						
(Server Core installation)	Security Update		Disclosure		Vector: CVSS: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	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0894						
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008	4089229	Important	Information	4074588	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0894						
for x64-based Systems Service Pack 2 (Server Core installation)	Security Update		Disclosure		Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	

CVE-2018-0895 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0895 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	kernel handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0895						
Product	**KB**	**Severity**	**Impact**	**Supersedenc**	**CVSS Score Set**	**Restart**

CVE-2018-0895						
	Article			**e**		**Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for	4088878 Security	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2018-0895						
x64-based Systems Service Pack 1 (Server Core installation)	Only 4088875 Monthly Rollup				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0895						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0895						
	Security Only					
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4088876	Important	Information	4074594	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0895						
R2	Monthly Rollup 4088879 Security Only		Disclosure		Vector: CVSS: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 RT 8.1	4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit	4088786	Important	Information	4074596	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0895						
Systems	Security Update		Disclosure		Vector: CVSS: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	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0895						
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based	4088782 Security	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2018-0895						
Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0895						
Windows Server 2008 for 32-bit Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0896 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0896 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0896						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0896						
	Monthly Rollup					
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008	4088878	Important	Information	4074598	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0896						
R2 for Itanium-Based Systems Service Pack 1	Security Only 4088875 Monthly Rollup		Disclosure		Vector: CVSS: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	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0896						
Windows Server 2012	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 408887	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0896						
	9 Security Only					
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT	408887	Importan	Informatio	4074594	Base: 4.7	Yes

CVE-2018-0896						
8.1	6 Monthly Rollup	t	n Disclosure		Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0896						
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based	4088787 Security	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2018-0896						
Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10	408877	Importan	Informatio	4074588	Base: 4.7	Yes

CVE-2018-0896						
Version 1709 for x64-based Systems	6 Security Update	t	n Disclosure		Temporal: 4.2 Vector: CVSS: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, version 1709 (Server Core Installation)	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based	4089229 Security	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2018-0896						
Systems Service Pack 2	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0897 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0897 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0897						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008	4088878	Important	Information	4074598	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0897						
R2 for x64-based Systems Service Pack 1 (Server Core installation)	Security Only 4088875 Monthly Rollup		Disclosure		Vector: CVSS: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 Itanium-Based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0897						
	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 408888	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0897						
	0 Security Only					
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows	408887	Importan	Informatio	4074594	Base: 4.7	Yes

CVE-2018-0897						
Server 2012 R2	6 Monthly Rollup 4088879 Security Only	t	n Disclosure		Temporal: 4.2 Vector: CVSS: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 RT 8.1	4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10	408878	Importan	Informatio	4074596	Base: 4.7	Yes

CVE-2018-0897						
for 32-bit Systems	6 Security Update	t	n Disclosure		Temporal: 4.2 Vector: CVSS: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	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0897						
					C	
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703	4088782	Important	Information	4074592	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0897						
for x64-based Systems	Security Update		Disclosure		Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0897						
Service Pack 2						
Windows Server 2008 for 32-bit Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0898 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0898 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0898						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0898						
	Monthly Rollup					
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008	4088878	Important	Information	4074598	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0898						
R2 for Itanium-Based Systems Service Pack 1	Security Only 4088875 Monthly Rollup		Disclosure		Vector: CVSS: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	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0898						
Windows Server 2012	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 408887	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0898						
	9 Security Only					
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT	408887	Importan	Informatio	4074594	Base: 4.7	Yes

CVE-2018-0898						
8.1	6 Monthly Rollup	t	n Disclosure		Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0898						
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based	4088787 Security	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2018-0898						
Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10	408877	Importan	Informatio	4074588	Base: 4.7	Yes

CVE-2018-0898						
Version 1709 for x64-based Systems	6 Security Update	t	n Disclosure		Temporal: 4.2 Vector: CVSS: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, version 1709 (Server Core Installation)	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based	4089229 Security	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2018-0898						
Systems Service Pack 2	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0899 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0899 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0899						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008	4088878	Important	Information	4074598	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0899						
R2 for x64-based Systems Service Pack 1 (Server Core installation)	Security Only 4088875 Monthly Rollup		Disclosure		Vector: CVSS: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 Itanium-Based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0899						
	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 408888	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0899						
	0 Security Only					
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows	408887	Importan	Informatio	4074594	Base: 4.7	Yes

CVE-2018-0899						
Server 2012 R2	6 Monthly Rollup 4088879 Security Only	t	n Disclosure		Temporal: 4.2 Vector: CVSS: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 RT 8.1	4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10	408878	Importan	Informatio	4074596	Base: 4.7	Yes

CVE-2018-0899						
for 32-bit Systems	6 Security Update	t	n Disclosure		Temporal: 4.2 Vector: CVSS: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	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0899						
					C	
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703	4088782	Important	Information	4074592	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0899						
for x64-based Systems	Security Update		Disclosure		Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0899						
Service Pack 2						
Windows Server 2008 for 32-bit Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0900 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0900 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0900						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0900						
	Monthly Rollup					
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008	4088878	Important	Information	4074598	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0900						
R2 for Itanium-Based Systems Service Pack 1	Security Only 4088875 Monthly Rollup		Disclosure		Vector: CVSS: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	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0900						
Windows Server 2012	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 408887	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0900						
	9 Security Only					
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT	408887	Importan	Informatio	4074594	Base: 4.7	Yes

CVE-2018-0900						
8.1	6 Monthly Rollup	t	n Disclosure		Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0900						
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based	4088787 Security	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2018-0900						
Systems	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10	408877	Importan	Informatio	4074588	Base: 4.7	Yes

CVE-2018-0900						
Version 1709 for x64-based Systems	6 Security Update	t	n Disclosure		Temporal: 4.2 Vector: CVSS: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, version 1709 (Server Core Installation)	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based	4089229 Security	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector:	Yes

CVE-2018-0900						
Systems Service Pack 2	Update				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0901 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0901 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0901						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008	4088878	Important	Information	4074598	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0901						
R2 for x64-based Systems Service Pack 1 (Server Core installation)	Security Only 4088875 Monthly Rollup		Disclosure		Vector: CVSS: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 Itanium-Based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0901						
	Rollup					
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 408888	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0901						
	0 Security Only					
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows	408887	Importan	Informatio	4074594	Base: 4.7	Yes

CVE-2018-0901						
Server 2012 R2	6 Monthly Rollup 4088879 Security Only	t	n Disclosure		Temporal: 4.2 Vector: CVSS: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 RT 8.1	4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10	408878	Importan	Informatio	4074596	Base: 4.7	Yes

CVE-2018-0901						
for 32-bit Systems	6 Security Update	t	n Disclosure		Temporal: 4.2 Vector: CVSS: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	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0901						
					C	
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703	4088782	Important	Information	4074592	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0901						
for x64-based Systems	Security Update		Disclosure		Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0901						
Service Pack 2					C	
Windows Server 2008 for x64-based Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0902 - CNG Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0902 MITRE	**CVE Title:** CNG Security Feature Bypass Vulnerability **Description:**	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
NVD	A security feature bypass vulnerability exists in the Cryptography Next Generation (CNG) kernel-mode driver (cng.sys) when it fails to properly validate and enforce impersonation levels. An attacker could exploit this vulnerability by convincing a user to run a specially crafted application that is designed to cause CNG to improperly validate impersonation levels, potentially allowing the attacker to gain access to information beyond the access level of the local user. The security update addresses the vulnerability by correcting how the kernel-mode driver validates and enforces impersonation levels. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0902						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Security Feature Bypass	4074596	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Security Feature Bypass	4074596	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Security Feature Bypass	4074591	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Security Feature Bypass	4074591	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

CVE-2018-0902						
Windows Server 2016	4088787 Security Update	Important	Security Feature Bypass	4074590	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Security Feature Bypass	4074590	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Security Feature Bypass	4074590	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Security Feature Bypass	4074590	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Security Feature Bypass	4074592	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based	4088782 Security Update	Important	Security Feature Bypass	4074592	Base: 5.3 Temporal: 4.8 Vector:	Yes

CVE-2018-0902						
Systems					CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Security Feature Bypass	4074588	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Security Feature Bypass	4074588	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Security Feature Bypass	4074588	Base: 5.3 Temporal: 4.8 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0903	**CVE Title:** Microsoft Access Remote Code Execution Vulnerability	Important	Remote Code

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	**Description:** A remote code execution vulnerability exists in Microsoft Access software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Access. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. The security update addresses the vulnerability by correcting how Microsoft Access handles objects in memory. **FAQ:** None **Mitigations:** None		Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0903						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Access 2010 Service Pack 2 (32-bit editions)	3114416 Security Update	Important	Remote Code Execution	3101544	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Access 2010 Service Pack 2	3114416 Security	Important	Remote Code	3101544	Base: N/A	Maybe

CVE-2018-0903						
(64-bit editions)	Update		Execution		Temporal: N/A Vector: N/A	
Microsoft Access 2016 (32-bit edition)	4011665 Security Update	Important	Remote Code Execution	2910978	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Access 2016 (64-bit edition)	4011665 Security Update	Important	Remote Code Execution	2910978	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Access 2013 Service Pack 1 (32-bit editions)	4011234 Security Update	Important	Remote Code Execution	3085584	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Access 2013 Service Pack 1 (64-bit editions)	4011234 Security Update	Important	Remote Code Execution	3085584	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Remote Code Execution	3085584	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2018-0903						
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Remote Code Execution	3085584	Base: N/A Temporal: N/A Vector: N/A	No

CVE-2018-0904 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0904 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (ASLR) bypass. An attacker who successfully exploited the vulnerability could retrieve the memory address of a kernel object. To exploit the vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0904						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0904						
Windows 7 for 32-bit Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems	4088878 Security Only 408887	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0904						
Service Pack 1 (Server Core installation)	5 Monthly Rollup					
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088878 Security Only 4088875 Monthly Rollup	Important	Information Disclosure	4074598	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows	408922	Importan	Informatio	4074598	Base: 4.7	Yes

CVE-2018-0904						
Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	9 Security Update	t	n Disclosure		Temporal: 4.2 Vector: CVSS: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	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4088877 Monthly Rollup 4088880 Security Only	Important	Information Disclosure	4074593	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0904						
Windows 8.1 for 32-bit systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0904						
	4088879 Security Only				C	
Windows RT 8.1	4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4088876 Monthly Rollup 4088879 Security Only	Important	Information Disclosure	4074594	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0904						
					C	
Windows 10 for x64-based Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607	4088787	Important	Information	4074590	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0904						
for 32-bit Systems	Security Update		Disclosure		Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0904						
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008	4089229	Important	Information	4074588	Base: 4.7 Temporal: 4.2	Yes

CVE-2018-0904						
for x64-based Systems Service Pack 2	Security Update		Disclosure		Vector: CVSS: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)	4089229 Security Update	Important	Information Disclosure	4074588	Base: 4.7 Temporal: 4.2 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0907 MITRE NVD	**CVE Title:** Microsoft Office Excel Security Feature Bypass **Description:** A security feature bypass vulnerability exists in Microsoft Office software by not enforcing macro settings on an Excel document. The security feature bypass by itself does not allow arbitrary code execution. To successfully exploit the	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	vulnerability, an attacker would have to embed a control in an Excel worksheet that specifies a macro should be run. Â To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted file with an affected version of Microsoft Office software. Â The security update addresses the vulnerability by enforcing macro settings on Excel documents. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0907						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Excel 2007 Service Pack 3	4011714 Security Update	Important	Security Feature Bypass	4011602	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	4011675 Security Update	Important	Security Feature Bypass	4011660	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	4011675 Security Update	Important	Security Feature Bypass	4011660	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	4018291 Security Update	Important	Security Feature Bypass	4011639	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0907						
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	4018291 Security Update	Important	Security Feature Bypass	4011639	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 RT Service Pack 1	4018291 Security Update	Important	Security Feature Bypass	4011639	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Security Feature Bypass	4011639	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Excel 2016 (32-bit edition)	4011727 Security Update	Important	Security Feature Bypass	4011627	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	4011727 Security Update	Important	Security Feature Bypass	4011627	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Security Feature Bypass	4011627	Base: N/A Temporal: N/A	No

CVE-2018-0907						
					Vector: N/A	
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Security Feature Bypass	4011627	Base: N/A Temporal: N/A Vector: N/A	No

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0909 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0909						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Project Server 2013 Service Pack 1	4018305 Security Update	Important	Elevation of Privilege	4011701	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4018293 Security Update	Important	Elevation of Privilege	4011680	Base: N/A Temporal: N/A Vector: N/A	Maybe

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0910 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0910						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0910						
Microsoft Project Server 2013 Service Pack 1	4018305 Security Update	Important	Elevation of Privilege	4011701	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4018293 Security Update	Important	Elevation of Privilege	4011680	Base: N/A Temporal: N/A Vector: N/A	Maybe

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0911 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0911						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Project Server 2013 Service Pack 1	4018305 Security Update	Important	Elevation of Privilege	4011701	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4018293 Security Update	Important	Elevation of Privilege	4011680	Base: N/A Temporal: N/A Vector: N/A	Maybe

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0912 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0912						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0912						
Microsoft Project Server 2013 Service Pack 1	4018305 Security Update	Important	Elevation of Privilege	4011701	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4018293 Security Update	Important	Elevation of Privilege	4011680	Base: N/A Temporal: N/A Vector: N/A	Maybe

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0913 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0913						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Project Server 2013 Service Pack 1	4018305 Security Update	Important	Elevation of Privilege	4011701	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4018293 Security Update	Important	Elevation of Privilege	4011680	Base: N/A Temporal: N/A Vector: N/A	Maybe

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0914 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0914						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0914						
Microsoft Project Server 2013 Service Pack 1	4018305 Security Update	Important	Elevation of Privilege	4011701	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4018293 Security Update	Important	Elevation of Privilege	4011680	Base: N/A Temporal: N/A Vector: N/A	Maybe

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0915 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0915						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Project Server 2013 Service Pack 1	4018305 Security Update	Important	Elevation of Privilege	4011701	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4018293 Security Update	Important	Elevation of Privilege	4011680	Base: N/A Temporal: N/A Vector: N/A	Maybe

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0916 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0916						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0916						
Microsoft Project Server 2013 Service Pack 1	4018305 Security Update	Important	Elevation of Privilege	4011701	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4018293 Security Update	Important	Elevation of Privilege	4011680	Base: N/A Temporal: N/A Vector: N/A	Maybe

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0917 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0917						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Enterprise Server 2016	4018293 Security Update	Important	Elevation of Privilege	4011680	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0919 - Microsoft Office Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0919 MITRE NVD	**CVE Title:** Microsoft Office Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Microsoft Office software reads out of bound memory due to an uninitialized variable, which could disclose the	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	contents of memory. An attacker who successfully exploited the vulnerability could view out of bound memory. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. The security update addresses the vulnerability by properly initializing the affected variable. **FAQ:** **I have Microsoft Word 2010 installed. Why am I not being offered the 4011673 update?** The 4011673 update only applies to systems running specific configurations of Microsoft Office 2010. Some configurations will not be offered the update. **I am being offered this update for software that is not specifically indicated as being affected in the Affected Software and Vulnerability Severity Ratings table. Why am I being offered this update?** When updates address vulnerable code that exists in a component that is shared between multiple Microsoft Office products or shared between multiple versions of the same Microsoft Office product, the update is considered to be applicable to all supported products and versions that contain the vulnerable component.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	For example, when an update applies to Microsoft Office 2007 products, only Microsoft Office 2007 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2007, Microsoft Excel 2007, Microsoft Visio 2007, Microsoft Compatibility Pack, Microsoft Excel Viewer, or any other Microsoft Office 2007 product that is not specifically listed in the Affected Software table. Furthermore, when an update applies to Microsoft Office 2010 products, only Microsoft Office 2010 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2010, Microsoft Excel 2010, Microsoft Visio 2010, Microsoft Visio Viewer, or any other Microsoft Office 2010 product that is not specifically listed in the Affected Software table. For more information on this behavior and recommended actions, see Microsoft Knowledge Base Article 830335. For a list of Microsoft Office products that an update may apply to, refer to the Microsoft Knowledge Base Article associated with the specific update. **Mitigations:** None **Workarounds:** None **Revision:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0919						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Server 2010 Service Pack 2	4011705 Security Update	Important	Information Disclosure	4011609	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011674 Security Update	Important	Information Disclosure	4011659	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0919						
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4011674 Security Update	Important	Information Disclosure	4011659	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011673 Security Update	Important	Information Disclosure	4011658	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011673 Security Update	Important	Information Disclosure	4011658	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps 2010 Service Pack 2	4011709 Security Update	Important	Information Disclosure	4011615	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (32-bit editions)	4011695 Security Update	Important	Information Disclosure	4011651	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 Service Pack 1 (64-bit editions)	4011695 Security Update	Important	Information Disclosure	4011651	Base: N/A Temporal: N/A	Maybe

CVE-2018-0919						
					Vector: N/A	
Microsoft Word 2013 RT Service Pack 1	4011695 Security Update	Important	Information Disclosure	4011651	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps Server 2013 Service Pack 1	4011692 Security Update	Important	Information Disclosure	4011648	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 for Mac	Release Notes Security Update	Important	Information Disclosure	4011648	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Word 2016 (32-bit edition)	4011730 Security Update	Important	Information Disclosure	4011643	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2016 (64-bit edition)	4011730 Security Update	Important	Information Disclosure	4011643	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Online Server 2016	4011023 Security	Important	Information	4011022	Base: N/A	Maybe

CVE-2018-0919						
	Update		Disclosure		Temporal: N/A Vector: N/A	
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions	Click to Run Security Update	Important	Information Disclosure	4011022	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions	Click to Run Security Update	Important	Information Disclosure	4011022	Base: N/A Temporal: N/A Vector: N/A	No
Microsoft SharePoint Enterprise Server 2016	4018293 Security Update	Important	Information Disclosure	4011680	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4011688 Security Update	Important	Information Disclosure	4011579	Base: N/A Temporal: N/A Vector: N/A	Maybe

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0921 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0921						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0921						
Microsoft SharePoint Enterprise Server 2016	4018293 Security Update	Important	Elevation of Privilege	4011680	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0922 - Microsoft Office Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0922 MITRE NVD	**CVE Title:** Microsoft Office Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the Office software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	with an affected version of Microsoft Office software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. Note that the Preview Pane is not an attack vector for this vulnerability. The security update addresses the vulnerability by correcting how Office handles objects in memory. **FAQ:** **I have Microsoft Word 2010 installed. Why am I not being offered the 4011673 update?** The 4011673 update only applies to systems running specific configurations of Microsoft Office 2010. Some configurations will not be offered the update. **I am being offered this update for software that is not specifically indicated as being affected in the Affected Software and Vulnerability Severity Ratings**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	table. Why am I being offered this update? When updates address vulnerable code that exists in a component that is shared between multiple Microsoft Office products or shared between multiple versions of the same Microsoft Office product, the update is considered to be applicable to all supported products and versions that contain the vulnerable component. For example, when an update applies to Microsoft Office 2007 products, only Microsoft Office 2007 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2007, Microsoft Excel 2007, Microsoft Visio 2007, Microsoft Compatibility Pack, Microsoft Excel Viewer, or any other Microsoft Office 2007 product that is not specifically listed in the Affected Software table. Furthermore, when an update applies to Microsoft Office 2010 products, only Microsoft Office 2010 may be specifically listed in the Affected Software table. However, the update could apply to Microsoft Word 2010, Microsoft Excel 2010, Microsoft Visio 2010, Microsoft Visio Viewer, or any other Microsoft Office 2010 product that is not specifically listed in the Affected Software table. For more information on this behavior and recommended actions, see Microsoft Knowledge Base Article 830335. For a list of Microsoft Office products that an update may apply to, refer to the Microsoft Knowledge Base Article associated with the specific update.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Why is there a separate update for Word Viewer The Word Viewer update (4018309) is only supported, and will only install from Microsoft Update, if itâ€™s on Windows Embedded POSReady 2009. This is because Word Viewer ships pre-installed in Windows Embedded POSReady 2009, which is still in support. For other platforms, Word Viewer is no longer supported. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0922						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Word 2007 Service Pack 3	4011721 Security Update	Important	Remote Code Execution	4011657	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 (32-bit editions)	4011695 Security Update	Important	Remote Code Execution	4011651	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 (64-bit editions)	4011695 Security Update	Important	Remote Code Execution	4011651	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Server 2010 Service Pack 2	4011705 Security Update	Important	Remote Code Execution	4011609	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2010 Service Pack 2 (32-bit editions)	4011674 Security Update	Important	Remote Code Execution	4011659	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0922						
Microsoft Word 2010 Service Pack 2 (64-bit editions)	4011674 Security Update	Important	Remote Code Execution	4011659	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	4011673 Security Update	Important	Remote Code Execution	4011658	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	4011673 Security Update	Important	Remote Code Execution	4011658	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps 2010 Service Pack 2	4011709 Security Update	Important	Remote Code Execution	4011615	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Word 2013 RT Service Pack 1	4011695 Security Update	Important	Remote Code Execution	4011651	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps 2013 Service Pack 1	4011692 Security Update	Important	Remote Code Execution	4011648	Base: N/A Temporal: N/A	Maybe

CVE-2018-0922						
					Vector: N/A	
Microsoft Office Online Server 2016	4011023 Security Update	Important	Remote Code Execution	4011022	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4011688 Security Update	Important	Remote Code Execution	4011579	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Word Viewer	4018309 Security Update	Important	Remote Code Execution	4011641	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Compatibility Pack Service Pack 3	4011720 Security Update	Important	Remote Code Execution	4011607	Base: N/A Temporal: N/A Vector: N/A	Maybe

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0923 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0923						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**

CVE-2018-0923						
Microsoft SharePoint Enterprise Server 2016	4018293 Security Update	Important	Elevation of Privilege	4011680	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2013 Service Pack 1	4018298 Security Update	Important	Elevation of Privilege	4011170	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0924 - Microsoft Exchange Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0924 MITRE NVD	**CVE Title:** Microsoft Exchange Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that Microsoft Exchange Server handles URL redirects. If an impacted user is using Microsoft Exchange Outlook Web Access (OWA) Light, the vulnerability could allow an attacker to	Low	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	discover sensitive information that should otherwise not be disclosed, such as the URL of the user's OWA service. To exploit the vulnerability, an attacker could embed a link in an email and send it to a victim. The attacker would then have to trick the user into clicking the link. The attacker would be unable to force the user to click the link. The security update addresses the vulnerability by correcting how Microsoft Exchange handles URL redirects. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0924						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Exchange Server 2013 Service Pack 1	4073392 Security Update	Low	Information Disclosure	4036108	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2016 Cumulative Update 7	4073392 Security Update	Low	Information Disclosure	4045655	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2013 Cumulative Update 18	4073392 Security Update	Low	Information Disclosure	4045655	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2016 Cumulative Update 8	4073392 Security Update	Low	Information Disclosure	4045655	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0924						
Microsoft Exchange Server 2013 Cumulative Update 19	4073392 Security Update	Low	Information Disclosure	4045655	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 20	4073537 Security Update	Low	Information Disclosure	4035162	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0925 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0925 MITRE 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.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The security update addresses the vulnerability by modifying how the ChakraCore scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0925						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
ChakraCore	Commit Security Only	Critical	Remote Code Execution		Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O	Yes

CVE-2018-0926 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0926 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit this vulnerability, an authenticated attacker could run a specially crafted application. An attacker who successfully exploited this vulnerability could obtain information to further compromise the userâ€™s system. The update addresses the vulnerability by correcting how the Windows kernel initializes objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0926						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows Server 2016	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server	4088787 Security	Important	Information Disclosure	4074590	Base: 5.5 Temporal: 5	Yes

CVE-2018-0926						
2016 (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 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based	4088776 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0926						
Systems						
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Information Disclosure	4074588	Base: 5.5 Temporal: 5 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0927 - Microsoft Browser Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0927 MITRE NVD	**CVE Title:** Microsoft Browser Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when affected Microsoft browsers improperly handle objects in memory. An attacker who successfully exploited this	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	vulnerability could obtain information to further compromise the userâ€™s system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by modifying how Microsoft browsers handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00		

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-2018-0927						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service	4088875 Monthly Rollup 4089187 IE Cumulative	Important	Information Disclosure	4074736	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0927						
Pack 1						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4088875 Monthly Rollup 4089187 IE Cumulative	Important	Information Disclosure	4074736	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088875 Monthly Rollup 4089187 IE Cumulative	Low	Information Disclosure	4074736	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer	4089187 IE Cumulativ	Important	Information	4074594	Base: 4.3 Temporal: 3.9	Yes

CVE-2018-0927						
11 on Windows 8.1 for 32-bit systems	e 4088876 Monthly Rollup		Disclosure		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 8.1 for x64-based systems	4089187 IE Cumulative 4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4089187 IE Cumulative 4088876 Monthly Rollup	Low	Information Disclosure	4074594	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0927						
RT 8.1					C	
Internet Explorer 11 on Windows 10 for 32-bit Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for x64-base	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0927						
d Systems						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4088787 Security Update	Low	Information Disclosure	4074590	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0927						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2018-0927						
Windows 10 Version 1703 for x64-based Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-base	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0927						
d Systems						
Internet Explorer 10 on Windows Server 2012	4088877 Monthly Rollup 4089187 IE Cumulative	Low	Information Disclosure	4074736	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for 32-bit Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2018-0927						
10 Version 1511 for x64-based Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4088787 Security Update	Low	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0927						
1607 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0927						
Version 1703 for x64-based Systems					C	
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0929 - Internet Explorer Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0929 MITRE NVD	**CVE Title:** Internet Explorer Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory. **FAQ:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0929						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet	4089187 IE	Low	Informatio	4074736	Base: 2.4	Yes

CVE-2018-0929						
Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	Cumulative		n Disclosure		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	
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4089187 IE Cumulative	Low	Information Disclosure	4074736	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4088875 Monthly Rollup 4089187 IE	Important	Information Disclosure	4074736	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0929						
7 for 32-bit Systems Service Pack 1	Cumulative				C	
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4088875 Monthly Rollup 4089187 IE Cumulative	Important	Information Disclosure	4074736	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems	4088875 Monthly Rollup 4089187 IE Cumulative	Low	Information Disclosure	4074736	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0929						
Service Pack 1						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4089187 IE Cumulative 4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4089187 IE Cumulative 4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4089187 IE Cumulative 4088876 Monthly Rollup	Low	Information Disclosure	4074594	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0929						
Internet Explorer 11 on Windows RT 8.1	4088876 Monthly Rollup	Important	Information Disclosure	4074594	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4088786 Security Update	Important	Information Disclosure	4074596	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0929						
10 Version 1511 for x64-based Systems					C	
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Information Disclosure	4074591	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4088787 Security Update	Low	Information Disclosure	4074590	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2018-0929						
Windows 10 Version 1607 for 32-bit Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0929						
Systems						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Information Disclosure	4074592	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4088776 Security Update	Important	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0929						
10 Version 1709 for x64-based Systems					C	
Internet Explorer 10 on Windows Server 2012	4088877 Monthly Rollup 4089187 IE Cumulative	Low	Information Disclosure	4074736	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0930	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability	Critical	Remote Code

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0930						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2018-0930						
Version 1709 for 32-bit Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0931 MITRE 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	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	exploit the vulnerability. The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0931						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4088786 Security Update	Critical	Remote Code Execution	4074596	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4088786 Security Update	Critical	Remote Code Execution	4074596	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2018-0931						
Version 1511 for 32-bit Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows Server 2016	4088787 Security Update	Moderate	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft	4088782	Critical	Remote	4074592	Base: 4.2	Yes

CVE-2018-0931						
Edge on Windows 10 Version 1703 for 32-bit Systems	Security Update		Code Execution		Temporal: 3.8 Vector: CVSS: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 x64-based Systems	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2018-0931						
Version 1709 for x64-based Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0932 - Microsoft Browser Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0932 MITRE NVD	**CVE Title:** Microsoft Browser Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when affected Microsoft browsers improperly handle objects in memory. An attacker who successfully exploited this	Critical	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	vulnerability could obtain information to further compromise the userâ€™s system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by modifying how Microsoft browsers handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00		

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-2018-0932						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service	4088875 Monthly Rollup 4089187 IE Cumulative	Critical	Information Disclosure	4074736	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0932						
Pack 1						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4088875 Monthly Rollup 4089187 IE Cumulative	Critical	Information Disclosure	4074736	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088875 Monthly Rollup 4089187 IE Cumulative	Moderate	Information Disclosure	4074736	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer	4089187 IE Cumulativ	Critical	Information	4074594	Base: 4.3 Temporal: 3.9	Yes

CVE-2018-0932						
11 on Windows 8.1 for 32-bit systems	e 4088876 Monthly Rollup		Disclosure		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 8.1 for x64-based systems	4089187 IE Cumulative 4088876 Monthly Rollup	Critical	Information Disclosure	4074594	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4089187 IE Cumulative 4088876 Monthly Rollup	Moderate	Information Disclosure	4074594	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4088876 Monthly Rollup	Critical	Information Disclosure	4074594	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0932						
RT 8.1					C	
Internet Explorer 11 on Windows 10 for 32-bit Systems	4088786 Security Update	Critical	Information Disclosure	4074596	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4088786 Security Update	Critical	Information Disclosure	4074596	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for x64-base	4088779 Security Update	Critical	Information Disclosure	4074591	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0932						
d Systems						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Critical	Information Disclosure	4074591	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4088787 Security Update	Moderate	Information Disclosure	4074590	Base: 2.4 Temporal: 2.2 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4088787 Security Update	Critical	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0932						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Critical	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Critical	Information Disclosure	4074592	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4088782 Security Update	Critical	Information Disclosure	4074592	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2018-0932						
Windows 10 Version 1703 for x64-based Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Critical	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1709 for x64-base	4088776 Security Update	Critical	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0932						
d Systems						
Microsoft Edge on Windows 10 for 32-bit Systems	4088786 Security Update	Critical	Information Disclosure	4074596	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4088786 Security Update	Critical	Information Disclosure	4074596	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Critical	Information Disclosure	4074591	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on	4088779 Security	Critical	Information	4074591	Base: 4.3 Temporal: 3.9	Yes

CVE-2018-0932						
Windows 10 Version 1511 for 32-bit Systems	Update		Disclosure		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	
Microsoft Edge on Windows Server 2016	4088787 Security Update	Moderate	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Critical	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10	4088787 Security Update	Critical	Information Disclosure	4074590	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:	Yes

CVE-2018-0932						
Version 1607 for x64-based Systems					C	
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Critical	Information Disclosure	4074592	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Critical	Information Disclosure	4074592	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4088776 Security Update	Critical	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector:	Yes

CVE-2018-0932						
10 Version 1709 for 32-bit Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Critical	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0933 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. **FAQ:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0933						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on	4088786 Security	Critical	Remote Code	4074596	Base: 4.2 Temporal: 3.8	Yes

CVE-2018-0933						
Windows 10 for 32-bit Systems	Update		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 for x64-based Systems	4088786 Security Update	Critical	Remote Code Execution	4074596	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0933						
Microsoft Edge on Windows Server 2016	4088787 Security Update	Moderate	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0933						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0933						
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0934 MITRE 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how the Chakra scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0934						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 for 32-bit Systems	4088786 Security Update	Critical	Remote Code Execution	4074596	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4088786 Security Update	Critical	Remote Code Execution	4074596	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0934						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Critical	Remote Code Execution	4074591	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows Server 2016	4088787 Security Update	Moderate	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10	4088787 Security Update	Critical	Remote Code Execution	4074590	Base: 4.2 Temporal: 3.8 Vector:	Yes

CVE-2018-0934						
Version 1607 for x64-based Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0934						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0935 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0935 MITRE	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Important	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0935						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 9	4089187 IE Cumulative	Low	Remote Code	4074736	Base: 6.4 Temporal: 5.8	Yes

CVE-2018-0935						
on Windows Server 2008 for 32-bit Systems Service Pack 2			Execution		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 9 on Windows Server 2008 for x64-based Systems Service Pack 2	4089187 IE Cumulative	Low	Remote Code Execution	4074736	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for	4088875 Monthly Rollup 4089187 IE Cumulative	Important	Remote Code Execution	4074736	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0935						
32-bit Systems Service Pack 1						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4088875 Monthly Rollup 4089187 IE Cumulative	Important	Remote Code Execution	4074736	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service	4088875 Monthly Rollup 4089187 IE Cumulative	Low	Remote Code Execution	4074736	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0935						
Pack 1						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4089187 IE Cumulative 4088876 Monthly Rollup	Important	Remote Code Execution	4074594	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4089187 IE Cumulative 4088876 Monthly Rollup	Important	Remote Code Execution	4074594	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4089187 IE Cumulative 4088876 Monthly Rollup	Low	Remote Code Execution	4074594	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer	4088876 Monthly	Important	Remote Code	4074594	Base: 7.5 Temporal: 6.7	Yes

CVE-2018-0935						
11 on Windows RT 8.1	Rollup		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 for 32-bit Systems	4088786 Security Update	Important	Remote Code Execution	4074596	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4088786 Security Update	Important	Remote Code Execution	4074596	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4088779 Security Update	Important	Remote Code Execution	4074591	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0935						
1511 for x64-based Systems						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Remote Code Execution	4074591	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4088787 Security Update	Low	Remote Code Execution	4074590	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10	4088787 Security Update	Important	Remote Code Execution	4074590	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0935						
Version 1607 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Remote Code Execution	4074590	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Remote Code Execution	4074592	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet	4088782	Important	Remote	4074592	Base: 7.5	Yes

CVE-2018-0935						
Explorer 11 on Windows 10 Version 1703 for x64-based Systems	Security Update		Code Execution		Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Remote Code Execution	4074588	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4088776 Security Update	Important	Remote Code Execution	4074588	Base: 7.5 Temporal: 6.7 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0935						
1709 for x64-based Systems						
Internet Explorer 10 on Windows Server 2012	4088877 Monthly Rollup 4089187 IE Cumulative	Low	Remote Code Execution	4074736	Base: 6.4 Temporal: 5.8 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0936 MITRE 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	Critical	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0936						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0936						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Only	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0937 MITRE	**CVE Title:** Chakra Scripting Engine Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0937						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0937						
for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Critical	Remote Code Execution	4074592	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Critical	Remote Code Execution	4074588	Base: 4.2 Temporal: 3.8 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit	Critical	Remote	4074588	Base: 4.2	Yes

CVE-2018-0937						
	Security Only		Code Execution		Temporal: 3.8 Vector: CVSS: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-2018-0939 - Scripting Engine Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0939 MITRE NVD	**CVE Title:** Scripting Engine Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge. An attacker who successfully exploited the vulnerability could obtain information to further compromise the userâ€™s system. In a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability. In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability. However, in all cases an attacker would have no way to force a user to view the attacker-controlled content. Instead, an attacker would have to convince a user to take action. For example, an attacker could trick a user	Critical	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	into clicking a link that takes the user to the attacker's site. The security update addresses the vulnerability by changing how the scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0939						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Critical	Information Disclosure	4074592	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Critical	Information Disclosure	4074592	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Critical	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0939						
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Critical	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
ChakraCore	Commit Security Only	Critical	Information Disclosure	4074588	Base: 4.3 Temporal: 3.9 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0940 MITRE NVD	**CVE Title:** Microsoft Exchange Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft Exchange Outlook Web Access (OWA) fails to properly sanitize links presented to users. An attacker who	Moderate	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	successfully exploited this vulnerability could override the OWA interface with a fake login page and attempt to trick the user into disclosing sensitive information. To exploit the vulnerability, an attacker could send a specially crafted email message containing a malicious link to a user. The user would have to click the malicious link in order to be susceptible to the vulnerability. The security update addresses the vulnerability by correcting how Microsoft Exchange rewrites links presented within the body of emails. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0940						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Exchange Server 2013 Service Pack 1	4073392 Security Update	Moderate	Elevation of Privilege	4036108	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2016 Cumulative Update 7	4073392 Security Update	Moderate	Elevation of Privilege	4045655	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2013 Cumulative Update 18	4073392 Security Update	Moderate	Elevation of Privilege	4045655	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2016 Cumulative Update 8	4073392 Security Update	Moderate	Elevation of Privilege	4045655	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0940						
Microsoft Exchange Server 2013 Cumulative Update 19	4073392 Security Update	Moderate	Elevation of Privilege	4045655	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 20	4073537 Security Update	Important	Elevation of Privilege	4035162	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0941 - Microsoft Exchange Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0941 MITRE NVD	**CVE Title:** Microsoft Exchange Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the way that Microsoft Exchange Server handles importing data. If an impacted user is using Microsoft Exchange Outlook Web Access (OWA), the vulnerability could allow an attacker to discover	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	sensitive information that should otherwise not be disclosed. To exploit the vulnerability, an attacker would have to upload a specially crafted file to Microsoft Exchange Outlook Web Access (OWA). The security update addresses the vulnerability by correcting how Microsoft Exchange handles importing data. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0941						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Exchange Server 2016 Cumulative Update 7	4073392 Security Update	Important	Information Disclosure	4045655	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2016 Cumulative Update 8	4073392 Security Update	Important	Information Disclosure	4045655	Base: N/A Temporal: N/A Vector: N/A	Maybe

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0942 MITRE NVD	**CVE Title:** Internet Explorer Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Internet Explorer fails a check, allowing sandbox escape. An attacker who successfully exploited the vulnerability could use the sandbox escape to elevate privileges on an affected system. This vulnerability by itself does not allow arbitrary code execution; however, it could allow arbitrary code to be run if the attacker uses it in combination with another vulnerability (such as a remote code execution vulnerability or another elevation of privilege vulnerability) that is capable of leveraging the elevated privileges when code execution is attempted. The update addresses the vulnerability by correcting how Internet Explorer handles zone and integrity settings. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:**	Low	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0942						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Internet Explorer 11 on Windows 7 for 32-bit Systems Service	4088875 Monthly Rollup 4089187 IE Cumulative	Important	Elevation of Privilege	4074736	Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0942						
Pack 1						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4088875 Monthly Rollup 4089187 IE Cumulative	Important	Elevation of Privilege	4074736	Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4088875 Monthly Rollup 4089187 IE Cumulative	Low	Elevation of Privilege	4074736	Base: 2.6 Temporal: 2.4 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer	4089187 IE Cumulative	Important	Elevation of	4074594	Base: 3 Temporal: 2.7	Yes

CVE-2018-0942						
11 on Windows 8.1 for 32-bit systems	4088876 Monthly Rollup		Privilege		Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 8.1 for x64-based systems	4089187 IE Cumulative 4088876 Monthly Rollup	Important	Elevation of Privilege	4074594	Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4089187 IE Cumulative 4088876 Monthly Rollup	Low	Elevation of Privilege	4074594	Base: 2.6 Temporal: 2.4 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4088876 Monthly Rollup	Important	Elevation of Privilege	4074594	Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0942						
Internet Explorer 11 on Windows 10 for 32-bit Systems	4088786 Security Update	Important	Elevation of Privilege	4074596	Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4088786 Security Update	Important	Elevation of Privilege	4074596	Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Elevation of Privilege	4074591	Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0942						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Elevation of Privilege	4074591	Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4088787 Security Update	Low	Elevation of Privilege	4074590	Base: 2.6 Temporal: 2.4 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0942						
Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 3 Temporal: 2.7 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2018-0942						
10 Version 1703 for x64-based Systems						

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0944 MITRE NVD	**CVE Title:** Microsoft SharePoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0944						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft Project Server 2013 Service Pack 1	4018305 Security Update	Important	Elevation of Privilege	4011701	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft SharePoint Enterprise Server 2016	4018293 Security Update	Important	Elevation of Privilege	4011680	Base: N/A Temporal: N/A Vector: N/A	Maybe

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0947 MITRE NVD	**CVE Title:** Microsoft Sharepoint Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly verify tenant permissions. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could elevate permssions such that they gain full rights to the affected tenant. These attacks could allow the attacker to read content that the attacker is not authorized to read, change permissions, and edit or delete content. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly checks tenant permissions. **FAQ:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0947						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Microsoft SharePoint Foundation 2013 Service Pack 1	4018304 Security Update	Important	Elevation of Privilege	4011653	Base: N/A Temporal:	Maybe

CVE-2018-0947						
					N/A Vector: N/A	
Microsoft SharePoint Enterprise Server 2016	4018293 Security Update	Important	Elevation of Privilege	4011680	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2018-0977 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0977 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Windows kernel-mode driver handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0977						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 for 32-bit Systems	4088786 Security Update	Important	Elevation of Privilege	4074596	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4088786 Security Update	Important	Elevation of Privilege	4074596	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Elevation of Privilege	4074591	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4088779 Security Update	Important	Elevation of Privilege	4074591	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector:	Yes

CVE-2018-0977						
					CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 7 Temporal: 6.3 Vector:	Yes

CVE-2018-0977						
x64-based Systems					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 32-bit Systems	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server Core Installation)	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2018-0983 MITRE NVD	**CVE Title:** Windows Storage Services Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Storage Services improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context. To exploit the vulnerability, an attacker would first have to log on to the system, and then run a specially crafted application to take control over the affected system. The security update addresses the vulnerability by correcting how Storage Services handles objects in memory. **FAQ:** None **Mitigations:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 03/13/2018 07:00:00 Information published.		

Affected Software

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

CVE-2018-0983						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1511 for x64-based Systems	4088779 Security Update	Important	Elevation of Privilege	4074591	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10	4088779	Important	Elevation	4074591	Base: 7	Yes

CVE-2018-0983						
Version 1511 for 32-bit Systems	Security Update		of Privilege		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	
Windows Server 2016	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4088787 Security Update	Important	Elevation of Privilege	4074590	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10	4088782	Important	Elevation	4074592	Base: 7	Yes

CVE-2018-0983						
Version 1703 for 32-bit Systems	Security Update		of Privilege		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	
Windows 10 Version 1703 for x64-based Systems	4088782 Security Update	Important	Elevation of Privilege	4074592	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for 32-bit Systems	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1709 for x64-based Systems	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server, version 1709 (Server	4088776 Security Update	Important	Elevation of Privilege	4074588	Base: 7 Temporal: 6.3 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2018-0983						
Core Installation)						

声 明

==========

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

关于绿盟科技

==========

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

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

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

绿盟科技官方微博二维码

绿盟科技官方微信二维码