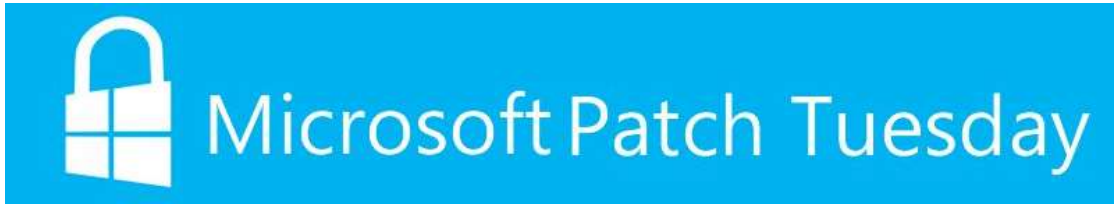
微软发布 7 月补丁修复 55 个安全问题

安全威胁通告



发布时间：2017 年 7 月 12 日

综述

微软于周二发布了 7 月安全更新补丁，修复了 55 个从简单的欺骗攻击到远程执行代码的安全问题，产品涉及 Internet Explorer、Microsoft Edge、Microsoft Windows、Microsoft Office 和 Microsoft Office Services and Web Apps、.NET Framework、Adobe Flash Player 以及 Microsoft Exchange Server。

相关信息如下（红色部分威胁相对比较高）：

产品	CVE ID	CVE 标题
.NET Framework	CVE-2017-8585	.NET 拒绝服务漏洞
Adobe Flash Player	ADV170009	7 月闪存安全更新
ASP .NET	CVE-2017-8582	Https.sys 信息泄露漏洞
HoloLens	CVE-2017-8584	HoloLens 远程执行代码漏洞
Internet Explorer	CVE-2017-8592	Microsoft 浏览器安全功能绕过漏洞
Internet Explorer	CVE-2017-8594	Internet Explorer 内存损坏漏洞

Internet Explorer	CVE-2017-8618	脚本引擎内存损坏漏洞
Kerberos	CVE-2017-8495	Kerberos SNAME 安全功能绕过漏洞
Microsoft Browsers	CVE-2017-8602	微软浏览器欺骗漏洞
Microsoft Edge	CVE-2017-8611	Microsoft Edge 欺骗漏洞
Microsoft Edge	CVE-2017-8596	Microsoft Edge 内存损坏漏洞
Microsoft Edge	CVE-2017-8617	Microsoft Edge 远程执行代码漏洞
Microsoft Edge	CVE-2017-8599	Microsoft Edge 安全功能绕过漏洞
Microsoft Edge	CVE-2017-8619	脚本引擎内存损坏漏洞
Microsoft Exchange Server	CVE-2017-8621	Microsoft Exchange 打开重定向漏洞
Microsoft Exchange Server	CVE-2017-8560	Microsoft Exchange 跨站脚本漏洞
Microsoft Exchange Server	CVE-2017-8559	Microsoft Exchange 跨站脚本漏洞
Microsoft Graphics Component	CVE-2017-8577	Win32k 提升特权漏洞
Microsoft Graphics Component	CVE-2017-8578	Win32k 提升特权漏洞
Microsoft Graphics Component	CVE-2017-8573	微软图形组件提升特权漏洞
Microsoft Graphics Component	CVE-2017-8574	微软图形组件提升特权漏洞
Microsoft Graphics Component	CVE-2017-8556	微软图形组件提升特权漏洞
Microsoft Graphics Component	CVE-2017-8580	Win32k 提升特权漏洞
Microsoft NTFS	CVE-2017-8587	Windows 资源管理器拒绝服务漏洞
Microsoft Office	CVE-2017-0243	Microsoft Office 远程执行代码漏洞
Microsoft Office	CVE-2017-8502	Microsoft Office 内存损坏漏洞
Microsoft Office	CVE-2017-8501	Microsoft Office 内存损坏漏洞
Microsoft Office	CVE-2017-8570	Microsoft Office 远程执行代码漏洞
Microsoft Office	CVE-2017-8569	SharePoint Server 跨站脚本漏洞
Microsoft PowerShell	CVE-2017-8565	Windows PowerShell 远程执行代码漏洞

Microsoft Scripting Engine	CVE-2017-8610	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8601	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8604	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8598	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8608	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8605	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8606	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8603	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8607	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8609	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8595	脚本引擎内存损坏漏洞
Microsoft Windows	CVE-2017-8557	Windows 控制台信息泄露漏洞
Microsoft Windows	CVE-2017-8566	Windows IME 提升特权漏洞
Microsoft Windows	CVE-2017-0170	Windows 性能监视器信息泄露漏洞
Microsoft Windows	CVE-2017-8590	Windows CLFS 提升特权漏洞
Microsoft Windows	CVE-2017-8562	Windows ALPC 特权提升漏洞
Microsoft Windows	CVE-2017-8589	Windows 搜索远程执行代码漏洞
Microsoft Windows	CVE-2017-8563	Windows 提升特权漏洞
Microsoft 写字板	CVE-2017-8588	写字板远程执行代码漏洞
Windows 内核	CVE-2017-8564	Windows 内核信息泄露漏洞
Windows 内核	CVE-2017-8561	Windows 内核提升特权漏洞
Windows 内核模式驱动程序	CVE-2017-8486	Win32k 信息泄露漏洞
Windows 内核模式驱动程序	CVE-2017-8467	Win32k 提升特权漏洞
Windows 内核模式驱动程序	CVE-2017-8581	Win32k 提升特权漏洞

Windows Shell	CVE-2017-8463	Windows 资源管理器远程执行代码漏洞

受影响的状况

见附件部分。

修复建议

微软官方已经发布更新补丁，请及时进行补丁更新。

附件

CVE-2017-0243 - Microsoft Office Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-	**CVE Title:** Microsoft Office Remote Code Execution Vulnerability **Description:**	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
0243 MITRE NVD	A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. Exploitation of this vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant Messenger message, and then convince the user to open the specially crafted file.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Microsoft Office handles files in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-0243						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required

CVE-2017-0243						
Microsoft Business Productivity Servers 2010 Service Pack 2	3203459 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2007 Service Pack 3	2880514 (Security Update)	Important	Remote Code Execution	2767772	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	3203468 (Security Update)	Important	Remote Code Execution	2956073	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	3203468 (Security Update)	Important	Remote Code Execution	2956073	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Web Apps 2010 Service Pack 2	3203469 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8569 - SharePoint Server XSS Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8569 MITRE NVD	**CVE Title:** SharePoint Server XSS Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run script in the security context of the current user. These attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user. The security update addresses the vulnerability by helping to ensure that SharePoint Server properly sanitizes web requests. **FAQ:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8569						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft SharePoint Enterprise Server 2016	3213544 (Security Update)	Important	Elevation of Privilege	3203432	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8570 - Microsoft Office Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8570 MITRE NVD	**CVE Title:** Microsoft Office Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when it fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could use a specially crafted file to perform actions in the security context of the current user. For example, the file could then take actions on behalf of the logged-on user with the same permissions as the current user. Exploitation of this vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file that is designed to exploit the vulnerability. However, an attacker would have no way to force the user to visit the website. Instead, an attacker would have to convince the user to click a link, typically by way of an enticement in an email or Instant	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Messenger message, and then convince the user to open the specially crafted file. The security update addresses the vulnerability by correcting how Microsoft Office handles files in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8570						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Office 2007 Service Pack 3	3213640 (Security Update)	Important	Remote Code Execution	3203436	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (32-bit editions)	3213624 (Security Update)	Important	Remote Code Execution	3203460	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2010 Service Pack 2 (64-bit editions)	3213624 (Security Update)	Important	Remote Code Execution	3203460	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 RT Service Pack 1	3213555 (Security Update)	Important	Remote Code Execution	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2013 Service Pack 1 (32-bit editions)	3213555 (Security Update)	Important	Remote Code Execution	3203386	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8570						
Microsoft Office 2013 Service Pack 1 (64-bit editions)	3213555 (Security Update)	Important	Remote Code Execution	3203386	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (32-bit edition)	3213545 (Security Update)	Important	Remote Code Execution	3191882	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 (64-bit edition)	3213545 (Security Update)	Important	Remote Code Execution	3191882	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8573 - Microsoft Graphics Component Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8573	**CVE Title:** Microsoft Graphics Component Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8573						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8573						
					CVSS: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 1511 for 32-bit Systems	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8573						
Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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 32-bit Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8573						
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8573						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8573						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025337 (Security Only) 4025341	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8573						
Service Pack 1	(Monthly Rollup)					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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)	4025331 (Monthly Rollup) 4025343	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8573						
	(Security Only)					
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8573						
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-2017-8574 - Microsoft Graphics Component Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8574 MITRE NVD	**CVE Title:** Microsoft Graphics Component Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Microsoft Graphics Component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses this vulnerability by correcting how the Microsoft Graphics Component handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8574						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8574						
Windows Server 2016	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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)	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8577 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8577 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Microsoft Graphics Component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Microsoft Graphics Component handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8577						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8577						
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-	4025342 (Securit	Important	Elevation of	4022725	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8577						
based Systems	y Update)		Privileg e		CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/R C:C	
Windows 7 for 32-bit Systems Service Pack 1	4025337 (Securit y Only) 4025341 (Monthly Rollup)	Importan t	Elevatio n of Privileg e	4022719	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/R C:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4025337 (Securit y Only) 4025341 (Monthly Rollup)	Importan t	Elevatio n of Privileg e	4022719	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/R C:C	Yes
Windows 8.1 for 32-bit systems	4025333 (Securit y Only) 4025336 (Monthly Rollup)	Importan t	Elevatio n of Privileg e	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/R C:C	Yes
Windows 8.1 for x64-	4025333 (Securit y Only)	Importan t	Elevatio n of	4022726	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8577						
based systems	4025336 (Monthly Rollup)		Privilege		CVSS: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 RT 8.1	4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown

CVE-2017-8577						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8577						
installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8577						
1 (Server Core installation)						
Windows Server 2012	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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)	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8577						
Windows Server 2012 R2 (Server Core installation)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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)	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8578 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8578 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Microsoft Graphics Component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The update addresses this vulnerability by correcting how the Microsoft Graphics Component handles objects in memory. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8578						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.70 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-2017-8578						
Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.70 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	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.70 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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.70 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-	4025339 (Securit	Important	Elevation of	4022715	Base: 7.00 Temporal: 6.70 Vector:	Yes

CVE-2017-8578						
based Systems	y Update)		Privilege		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	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.70 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	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.70 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 32-bit Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.70 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	4025337 (Security Only) 4025341	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.70 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-2017-8578						
Service Pack 1	(Monthly Rollup)					
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.70 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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: N/A Temporal: N/A Vector: N/A	Yes
Windows Server 2008 for 32-bit Systems	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 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-2017-8578						
Service Pack 2						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 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 for Itanium-Based Systems Service Pack 2	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 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 for x64-based Systems	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 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-2017-8578						
Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.70 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-	4025337 (Security Only)	Important	Elevation of	4022719	Base: 7.00 Temporal: 6.70 Vector:	Yes

CVE-2017-8578						
based Systems Service Pack 1	4025341 (Monthly Rollup)		Privilege		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 Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.70 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	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2012 (Server Core	4025331 (Monthly Rollup)	Important	Elevation of	4022724	Base: 7.00 Temporal: 6.70 Vector:	Yes

CVE-2017-8578						
installation)	4025343 (Security Only)		Privilege		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 Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.70 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)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.70 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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.70 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	4025339 (Securit	Important	Elevation of	4022715	Base: 7.00 Temporal: 6.70 Vector:	Yes

CVE-2017-8578						
installation)	y Update)		Privilege		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-2017-8580 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8580 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Microsoft Graphics Component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses this vulnerability by correcting how the Microsoft Graphics Component handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8580						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.70 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	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.70 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	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.70 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-2017-8580						
Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.70 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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.70 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	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	Yes
Windows 7 for 32-bit Systems	4025337 (Security Only) 4025341	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.70 Vector:	Yes

CVE-2017-8580						
Service Pack 1	(Monthly Rollup)				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 7 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.70 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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Elevation of	4022726	Base: 7.00 Temporal: 6.70 Vector:	Yes

CVE-2017-8580						
			Privilege		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 Server 2008 for 32-bit Systems Service Pack 2	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 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	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 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	Unknown
Windows Server 2008 for Itanium-Based Systems	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 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-2017-8580						
Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 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 for x64-based Systems Service Pack 2 (Server Core installation)	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-	4025337 (Security Only) 4025341	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.70 Vector:	Yes

CVE-2017-8580						
Based Systems Service Pack 1	(Monthly Rollup)				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 Server 2008 R2 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.70 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	4025331 (Monthly	Important	Elevation of	4022724	Base: 7.00 Temporal: 6.70	Yes

CVE-2017-8580						
	Rollup) 4025343 (Security Only)		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 Server 2012 (Server Core installation)	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.70 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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.70 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)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.70 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-2017-8580						
Windows Server 2016	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.70 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)	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.70 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-2017-8581 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8581 MITRE NVD	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows improperly handles objects in memory. An attacker who successfully exploited this vulnerability could run processes in an elevated context.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker would have to either log on locally to an affected system, or convince a locally authenticated user to execute a specially crafted application. The update addresses the vulnerability by correcting how the Windows kernel-mode driver handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8581						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes

CVE-2017-8581						
Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows 7 for 32-bit Systems	4025337 (Security Only)	Important	Elevation of	4022719	Base: 7.00 Temporal: 6.10 Vector:	Yes

CVE-2017-8581						
Service Pack 1	4025341 (Monthly Rollup)		Privilege		CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	
Windows 7 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows 8.1 for x64-based systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes

CVE-2017-8581						
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Unknown
Windows Server 2008 for Itanium-	4025877 (Securit	Important	Elevation of	None	Base: 7.00 Temporal: 6.10 Vector:	Yes

CVE-2017-8581						
Based Systems Service Pack 2	y Update)		Privilege		CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	
Windows Server 2008 for x64-based Systems Service Pack 2	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2008	4025337 (Securit	Important	Elevation of	4022719	Base: 7.00 Temporal: 6.10	Yes

CVE-2017-8581						
R2 for Itanium-Based Systems Service Pack 1	y Only) 4025341 (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:R	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes

CVE-2017-8581						
Windows Server 2012	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2012 (Server Core installation)	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2012 R2 (Server Core	4025333 (Security Only) 4025336	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes

CVE-2017-8581						
installation)	(Monthly Rollup)					
Windows Server 2016	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.10 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R	Yes
Windows Server 2016 (Server Core installation)	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	Yes

CVE-2017-8582 - Https.sys Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8582	**CVE Title:** Https.sys Information Disclosure Vulnerability **Description:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An Information Disclosure vulnerability exists when the HTTP.sys server application component improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the HTTP.sys server application system. A remote unauthenticated attacker could exploit this vulnerability by issuing a request to the HTTP.sys server application. The update addresses the vulnerability by correcting how the HTTP.sys server application handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8582						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Information Disclosure	4022727	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Information Disclosure	4022727	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Important	Information Disclosure	4022714	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes

CVE-2017-8582						
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Information Disclosure	4022714	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Information Disclosure	4022715	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Important	Information Disclosure	4022715	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Information Disclosure	4022725	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-	4025342 (Securit	Important	Information Disclosure	4022725	Base: 5.90 Temporal: 5.50 Vector:	Yes

CVE-2017-8582						
based Systems	y Update)				CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	
Windows 7 for 32-bit Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows 8.1 for x64-	4025333 (Security Only)	Important	Information Disclosure	4022726	Base: 5.90 Temporal: 5.50 Vector:	Yes

CVE-2017-8582						
based systems	4025336 (Monthly Rollup)				CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4022914 (Security Update)	Important	Information Disclosure	None	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4022914 (Security Update)	Important	Information Disclosure	None	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes

CVE-2017-8582						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4022914 (Security Update)	Important	Information Disclosure	None	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4022914 (Security Update)	Important	Information Disclosure	None	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core	4022914 (Security Update)	Important	Information Disclosure	None	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes

CVE-2017-8582						
installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes

CVE-2017-8582						
1 (Server Core installation)						
Windows Server 2012	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Information Disclosure	4022724	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Information Disclosure	4022724	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes

CVE-2017-8582						
Windows Server 2012 R2 (Server Core installation)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2016	4025339 (Security Update)	Important	Information Disclosure	4022715	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4025339 (Security Update)	Important	Information Disclosure	4022715	Base: 5.90 Temporal: 5.50 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C	Yes

CVE-2017-8584 - HoloLens Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8584 MITRE NVD	**CVE Title:** HoloLens Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when HoloLens improperly handles objects in memory. An attacker who successfully exploited this 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. To exploit this vulnerability, an attacker would need to send a specially crafted WiFi packet. The update addresses the vulnerability by correcting how Hololens handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8584						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 7.50 Temporal: 7.00 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-	4025339 (Securit	Critical	Remote Code	4022715	Base: 7.50 Temporal: 7.00 Vector:	Yes

CVE-2017-8584						
based Systems	y Update)		Executio n		CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/R C:C	
Windows Server 2016	4025339 (Securit y Update)	Critica l	Remote Code Executio n	4022715	Base: 7.50 Temporal: 7.00 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/R C:C	Yes
Windows Server 2016 (Server Core installation)	4025339 (Securit y Update)	Critica l	Remote Code Executio n	4022715	Base: 7.50 Temporal: 7.00 Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/R C:C	Yes

CVE-2017-8585 - .NET Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8585	**CVE Title:** .NET Denial of Service Vulnerability **Description:**	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A denial of service vulnerability exists when Microsoft Common Object Runtime Library improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against a .NET web application. A remote unauthenticated attacker could exploit this vulnerability by issuing specially crafted requests to the .NET application. The update addresses the vulnerability by correcting how the .NET web application handles web requests. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8585						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft .NET Framework 4.6 on Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Denial of Service	4022727	Base: 7.50 Temporal: 7.50 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Yes
Microsoft .NET Framework 4.6 on Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Denial of Service	4022727	Base: 7.50 Temporal: 7.50 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Yes
Microsoft .NET Framework 4.6.1 on Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Important	Denial of Service	4022714	Base: 7.50 Temporal: 7.50 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Yes
Microsoft .NET Framework 4.6.1 on Windows 10 Version	4025344 (Security Update)	Important	Denial of Service	4022714	Base: 7.50 Temporal: 7.50	Yes

CVE-2017-8585						
1511 for x64-based Systems					Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	
Microsoft .NET Framework 4.6.2/4.7 on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Denial of Service	4022715	Base: 7.50 Temporal: 7.50 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Yes
Microsoft .NET Framework 4.6.2/4.7 on Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Important	Denial of Service	4022715	Base: 7.50 Temporal: 7.50 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Yes
Microsoft .NET Framework 4.6.2/4.7 on Windows Server 2016	4025339 (Security Update)	Important	Denial of Service	4022715	Base: 7.50 Temporal: 7.50 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Yes
Microsoft .NET Framework 4.6.2/4.7 on Windows Server 2016 (Server Core installation)	4025339 (Security Update)	Important	Denial of Service	4022715	Base: 7.50 Temporal: 7.50 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Yes

CVE-2017-8585						
Microsoft .NET Framework 4.7 on Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Denial of Service	4022725	Base: 7.50 Temporal: 7.50 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Yes
Microsoft .NET Framework 4.7 on Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Denial of Service	4022725	Base: 7.50 Temporal: 7.50 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Yes

CVE-2017-8587 - Windows Explorer Denial of Service Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8587 MITRE NVD	**CVE Title:** Windows Explorer Denial of Service Vulnerability **Description:** An Denial Of Service vulnerability exists when Windows Explorer attempts to open a non-existent file.	Important	Denial of Service

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	An attacker who successfully exploited this vulnerability could cause a denial of service. A attacker could exploit this vulnerability by hosting a specially crafted web site and convince a user to browse to the page, containing the reference to the non-existing file, and cause the victim's system to stop responding. An attacker could not 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 correcting how Windows Explorer handles open attempts for non-existent files. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8587						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Denial of Service	4022727	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Denial of Service	4022727	Base: 6.50 Temporal: 6.00 Vector:	Yes

CVE-2017-8587						
					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	
Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Important	Denial of Service	4022714	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Denial of Service	4022714	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Denial of Service	4022719	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4025337 (Security Only) 4025341	Important	Denial of Service	4022719	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes

CVE-2017-8587						
Service Pack 1	(Monthly Rollup)					
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Denial of Service	4022726	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Denial of Service	4022726	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Denial of Service	4022726	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4025674 (Security Update)	Important	Denial of Service	2840149	Base: 6.50 Temporal: 6.00 Vector:	Yes

CVE-2017-8587						
Service Pack 2					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4025674 (Security Update)	Important	Denial of Service	2840149	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4025674 (Security Update)	Important	Denial of Service	2840149	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4025674 (Security Update)	Important	Denial of Service	2840149	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes

CVE-2017-8587						
Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4025674 (Security Update)	Important	Denial of Service	2840149	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Denial of Service	4022719	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4025337 (Security Only)	Important	Denial of	4022719	Base: 6.50 Temporal: 6.00 Vector:	Yes

CVE-2017-8587						
based Systems Service Pack 1	4025341 (Monthly Rollup)		Service		CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Denial of Service	4022719	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2012	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Denial of Service	4022724	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2012 (Server Core	4025331 (Monthly Rollup)	Important	Denial of	4022724	Base: 6.50 Temporal: 6.00 Vector:	Yes

CVE-2017-8587						
installation)	4025343 (Security Only)		Service		CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Denial of Service	4022726	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Denial of Service	4022726	Base: 6.50 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C	Yes

CVE-2017-8588 - WordPad Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8588 MITRE NVD	**CVE Title:** WordPad Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in the way that Microsoft WordPad parses specially crafted files. Exploitation of this vulnerability requires that a user open a specially crafted file with an affected version of Microsoft WordPad. In an email attack scenario, an attacker could exploit the vulnerability by sending a specially crafted file to the user and then convincing the user to open the file. The update addresses the vulnerability by correcting the way that Microsoft WordPad parses specially crafted files, and by enabling API functionality in Windows that Microsoft WordPad will leverage to resolve the identified issue. **FAQ:** None **Mitigations:** None	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8588						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Remote Code Execution	4022727	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/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-	4025338 (Securit	Important	Remote Code	4022727	Base: 6.70 Temporal: 6.00	Yes

CVE-2017-8588						
based Systems	y Update)		Executio n		Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1511 for 32-bit Systems	4025344 (Securit y Update)	Importan t	Remote Code Executio n	4022714	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/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	4025344 (Securit y Update)	Importan t	Remote Code Executio n	4022714	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/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	4025339 (Securit y Update)	Importan t	Remote Code Executio n	4022715	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/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	4025339 (Securit y Update)	Importan t	Remote Code Executio n	4022715	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8588						
Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Remote Code Execution	4022725	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Remote Code Execution	4022725	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Remote Code Execution	4022719	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/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	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Remote Code Execution	4022719	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8588						
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Remote Code Execution	4022726	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Remote Code Execution	4022726	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/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	4025336 (Monthly Rollup)	Important	Remote Code Execution	4022726	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/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	4026061 (Security Update)	Important	Remote Code Execution	None	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8588						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4026061 (Security Update)	Important	Remote Code Execution	None	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4026061 (Security Update)	Important	Remote Code Execution	None	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/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	4026061 (Security Update)	Important	Remote Code Execution	None	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8588						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4026061 (Security Update)	Important	Remote Code Execution	None	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/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	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Remote Code Execution	4022719	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems	4025337 (Security Only) 4025341	Important	Remote Code Execution	4022719	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8588						
Service Pack 1	(Monthly Rollup)					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Remote Code Execution	4022719	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Remote Code Execution	4022724	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4025331 (Monthly Rollup) 4025343	Important	Remote Code Execution	4022724	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8588						
	(Security Only)					
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Remote Code Execution	4022726	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/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)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Remote Code Execution	4022726	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4025339 (Security Update)	Important	Remote Code Execution	4022715	Base: 6.70 Temporal: 6.00 Vector: CVSS:3.0/AV:L/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	4025339 (Security Update)	Important	Remote Code Execution	4022715	Base: 6.70 Temporal: 6.00 Vector:	Yes

CVE-2017-8588						
installation)					CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	

CVE-2017-8589 - Windows Search Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8589 MITRE NVD	**CVE Title:** Windows Search Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Windows Search handles objects in memory. An attacker who successfully exploited this vulnerability 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. To exploit the vulnerability, the attacker could send specially crafted messages to the Windows Search service. An attacker with access to a target computer could exploit this vulnerability to elevate privileges and take control of the computer. Additionally, in an enterprise scenario, a remote unauthenticated attacker could remotely trigger the vulnerability through an SMB connection and then take control of a target computer.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how Windows Search handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8589						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required

CVE-2017-8589						
Windows 10 for 32-bit Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/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	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/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	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/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	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/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	4025339 (Securit	Critical	Remote Code	4022715	Base: 8.10 Temporal: 7.30 Vector:	Yes

CVE-2017-8589						
for 32-bit Systems	y Update)		Execution		CVSS:3.0/AV:N/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 x64-based Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/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	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Critical	Remote Code Execution	4022719	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8589						
Windows 7 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Critical	Remote Code Execution	4022719	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/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	4025333 (Security Only) 4025336 (Monthly Rollup)	Critical	Remote Code Execution	4022726	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/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 x64-based systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Critical	Remote Code Execution	4022726	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/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	4025336 (Monthly Rollup)	Critical	Remote Code Execution	4022726	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8589						
Windows Server 2008 for 32-bit Systems Service Pack 2	4032955 (Security Update)	Critical	Remote Code Execution	None	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/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)	4032955 (Security Update)	Critical	Remote Code Execution	None	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4032955 (Security Update)	Critical	Remote Code Execution	None	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8589						
Windows Server 2008 for x64-based Systems Service Pack 2	4032955 (Security Update)	Critical	Remote Code Execution	None	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/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)	4032955 (Security Update)	Critical	Remote Code Execution	None	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems	4025337 (Security Only) 4025341 (Monthly Rollup)	Critical	Remote Code Execution	4022719	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8589						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Critical	Remote Code Execution	4022719	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/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)	4025337 (Security Only) 4025341 (Monthly Rollup)	Critical	Remote Code Execution	4022719	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4025331 (Monthly Rollup) 4025343	Critical	Remote Code Execution	4022724	Base: 8.10 Temporal: 7.30 Vector:	Yes

CVE-2017-8589						
	(Security Only)				CVSS:3.0/AV:N/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)	4025331 (Monthly Rollup) 4025343 (Security Only)	Critical	Remote Code Execution	4022724	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/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	4025333 (Security Only) 4025336 (Monthly Rollup)	Critical	Remote Code Execution	4022726	Base: 8.10 Temporal: 8.10 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	Yes
Windows Server 2012 R2 (Server Core installation)	4025333 (Security Only) 4025336 (Monthly Rollup)	Critical	Remote Code Execution	4022726	Base: 8.10 Temporal: 8.10 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	Yes
Windows Server 2016	4025339 (Securit	Critical	Remote Code	4022715	Base: 8.10 Temporal: 7.30 Vector:	Yes

CVE-2017-8589						
	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 8.10 Temporal: 7.30 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8590 - Windows CLFS Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8590 MITRE NVD	**CVE Title:** Windows CLFS Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory. In a local attack scenario, an attacker could exploit this vulnerability by running a specially crafted application to take control of the affected	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	system. An attacker who successfully exploited this vulnerability could run processes in an elevated context. The update addresses the vulnerability by correcting how CLFS handles objects in memory. Note: The Common Log File System (CLFS) is a high-performance, general-purpose log file subsystem that dedicated client applications can use and multiple clients can share to optimize log access. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8590						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8590						
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-	4025342 (Securit	Important	Elevation of	4022725	Base: 8.80 Temporal: 7.90 Vector:	Yes

CVE-2017-8590						
based Systems	y Update)		Privileg e		CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/R C:C	
Windows 7 for 32-bit Systems Service Pack 1	4025337 (Securit y Only) 4025341 (Monthly Rollup)	Importan t	Elevatio n of Privileg e	4022719	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/R C:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4025337 (Securit y Only) 4025341 (Monthly Rollup)	Importan t	Elevatio n of Privileg e	4022719	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/R C:C	Yes
Windows 8.1 for 32-bit systems	4025333 (Securit y Only) 4025336 (Monthly Rollup)	Importan t	Elevatio n of Privileg e	4022726	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/R C:C	Yes
Windows 8.1 for x64-	4025333 (Securit y Only)	Importan t	Elevatio n of	4022726	Base: 8.80 Temporal: 7.90 Vector:	Yes

CVE-2017-8590						
based systems	4025336 (Monthly Rollup)		Privilege		CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4026059 (Security Update)	Important	Elevation of Privilege	3181707; 3203838	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/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)	4026059 (Security Update)	Important	Elevation of Privilege	3181707; 3203838	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8590						
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4026059 (Security Update)	Important	Elevation of Privilege	3181707; 3203838	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4026059 (Security Update)	Important	Elevation of Privilege	3181707; 3203838	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/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	4026059 (Security Update)	Important	Elevation of Privilege	3181707; 3203838	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8590						
installation)						
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8590						
1 (Server Core installation)						
Windows Server 2012	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8590						
Windows Server 2012 R2 (Server Core installation)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 8.80 Temporal: 7.90 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8592 - Microsoft Browser Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8592 MITRE NVD	**CVE Title:** Microsoft Browser Security Feature Bypass **Description:** A security feature bypass vulnerability exists when Microsoft Browsers improperly handle redirect requests. This vulnerability allows Microsoft Browsers to bypass CORS redirect restrictions and to follow redirect requests that should otherwise be ignored. An attacker who successfully exploited this vulnerability could force the browser to send data that would otherwise be restricted to a destination web site of their choice. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft browsers and then convince a user to view the website. The attacker could also take advantage of compromised websites, and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how affected Microsoft Browsers handle redirect requests. **FAQ:** None	Low	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8592						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Internet Explorer 10 on Windows Server 2012	4025331 (Monthly Rollup) 4025252 (IE	Low	Security Feature Bypass	4022724 4021558	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8592						
	Cumulative)					
Internet Explorer 11 on Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Security Feature Bypass	4022727	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Security Feature Bypass	4022727	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Important	Security Feature Bypass	4022714	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version	4025344 (Security Update)	Important	Security Feature Bypass	4022714	Base: 5.40 Temporal: 4.90 Vector:	Yes

CVE-2017-8592						
1511 for x64-based Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Security Feature Bypass	4022715	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Important	Security Feature Bypass	4022715	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Security Feature Bypass	4022725	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8592						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Security Feature Bypass	4022725	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4025341 (Monthly Rollup) 4025252 (IE Cumulative)	Important	Security Feature Bypass	4022719 4021558	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4025341 (Monthly Rollup) 4025252 (IE Cumulative)	Important	Security Feature Bypass	4022719 4021558	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8592						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Important	Security Feature Bypass	4022726 4021558	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Important	Security Feature Bypass	4022726 4021558	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4025336 (Monthly Rollup)	Important	Security Feature Bypass	4022726	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008	4025341 (Monthly Rollup) 4025252	Low	Security Feature Bypass	4022719 4021558	Base: 3.50 Temporal: 3.20 Vector:	Yes

CVE-2017-8592						
R2 for x64-based Systems Service Pack 1	(IE Cumulative)				CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows Server 2012 R2	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Low	Security Feature Bypass	4022726 4021558	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2016	4025339 (Security Update)	Low	Security Feature Bypass	4022715	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems	4025252 (IE Cumulative)	Low	Security Feature Bypass	4021558	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8592						
Service Pack 2						
Microsoft Edge on Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Security Feature Bypass	4022727	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/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	4025338 (Security Update)	Important	Security Feature Bypass	4022727	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR: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	4025344 (Security Update)	Important	Security Feature Bypass	4022714	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR: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	4025344 (Security Update)	Important	Security Feature Bypass	4022714	Base: 5.40 Temporal: 4.90 Vector:	Yes

CVE-2017-8592						
for x64-based Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Security Feature Bypass	4022727	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Security Feature Bypass	4022727	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Important	Security Feature Bypass	4022714	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Security Feature Bypass	4022714	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8592						
Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Security Feature Bypass	4022715	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Important	Security Feature Bypass	4022715	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Security Feature Bypass	4022719	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Security Feature Bypass	4022719	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8592						
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Security Feature Bypass	4022726	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Security Feature Bypass	4022726	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Security Feature Bypass	4022726	Base: 5.40 Temporal: 4.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4025240 (Security Update)	Important	Security Feature Bypass	3216916	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8592						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4025240 (Security Update)	Important	Security Feature Bypass	3216916	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4025240 (Security Update)	Important	Security Feature Bypass	3216916	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4025240 (Security Update)	Important	Security Feature Bypass	3216916	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8592						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4025240 (Security Update)	Important	Security Feature Bypass	3216916	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Security Feature Bypass	4022719	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Security Feature Bypass	4022719	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8592						
1 (Server Core installation)						
Windows Server 2012	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Security Feature Bypass	4022724	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Security Feature Bypass	4022724	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Security Feature Bypass	4022726	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8592						
Windows Server 2012 R2 (Server Core installation)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Security Feature Bypass	4022726	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4025339 (Security Update)	Important	Security Feature Bypass	4022715	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4025339 (Security Update)	Important	Security Feature Bypass	4022715	Base: 3.50 Temporal: 3.20 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8594 - Internet Explorer Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8594 MITRE NVD	**CVE Title:** Internet Explorer Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, the attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker could host a specially crafted website designed to exploit the vulnerability through Internet Explorer, and then convince a user to view the website. The attacker could also take advantage of compromised websites, or websites that accept or host user-provided content or advertisements, by adding specially crafted content that could exploit the vulnerability. 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	action, typically by an enticement in an email or instant message, or by getting them to open an attachment sent through email. The security update addresses the vulnerability by modifying how Internet Explorer handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8594						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Critical	Remote Code Execution	4022726 4021558	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/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	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Critical	Remote Code Execution	4022726 4021558	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explore	4025336 (Monthly Rollup)	Critical	Remote Code	4022726	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8594						
r 11 on Windows RT 8.1			Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows Server 2012 R2	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Moderate	Remote Code Execution	4022726 4021558	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8595 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8595 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way Microsoft Edge 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	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. In addition, an attacker could embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. Finally, the attacker could 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 Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8595						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Edge on Windows 10 for 32-bit Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8595						
Microsoft Edge on Windows 10 for x64-based Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8595						
1511 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8595						
Microsoft Edge on Windows Server 2016	4025339 (Security Update)	Moderate	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8596 - Microsoft Edge Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8596 MITRE NVD	**CVE Title:** Microsoft Edge Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way Microsoft Edge handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. In addition, an attacker could embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. Finally, the attacker could 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 Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8596						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8596						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8596						
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 Server 2016	4025339 (Security Update)	Moderate	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8617 - Microsoft Edge Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8617	**CVE Title:** Microsoft Edge Remote Code Execution Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists in the way Microsoft Edge handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. In addition, an attacker could embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. Finally, the attacker could 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 Microsoft Edge handles objects in memory.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8617						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Edge on	4025342 (Securit	Critical	Remote Code	4022725	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8617						
Windows 10 Version 1703 for 32-bit Systems	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8618 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8618 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the VBScript engine, when rendered in Internet Explorer, handles objects in memory. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit this 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 Internet Explorer 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 this vulnerability. An attacker who successfully exploited this 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 this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by modifying how the VBScript scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8618						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required

CVE-2017-8618						
Internet Explorer 10 on Windows Server 2012	4025331 (Monthly Rollup) 4025252 (IE Cumulative)	Moderate	Remote Code Execution	4022724 4021558	Base: 6.40 Temporal: 5.80 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 for 32-bit Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/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-	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8618						
based Systems						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for x64-	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8618						
based Systems						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/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-	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8618						
based Systems						
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for x64-	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8618						
based Systems						
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4025341 (Monthly Rollup) 4025252 (IE Cumulative)	Critical	Remote Code Execution	4022719 4021558	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/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	4025341 (Monthly Rollup) 4025252 (IE Cumulative)	Critical	Remote Code Execution	4022719 4021558	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8618						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Critical	Remote Code Execution	4022726 4021558	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/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	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Critical	Remote Code Execution	4022726 4021558	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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	4025336 (Monthly Rollup)	Critical	Remote Code Execution	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8618						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025341 (Monthly Rollup) 4025252 (IE Cumulative)	Moderate	Remote Code Execution	4022719 4021558	Base: 6.40 Temporal: 5.80 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 Server 2012 R2	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Moderate	Remote Code Execution	4022726 4021558	Base: 6.40 Temporal: 5.80 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 Explore	4025339 (Security Update)	Moderate	Remote Code	4022715	Base: 6.40 Temporal: 5.80 Vector:	Yes

CVE-2017-8618						
r 11 on Windows Server 2016			Execution		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 32-bit Systems Service Pack 2	4025252 (IE Cumulative)	Moderate	Remote Code Execution	4021558	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008	4025252 (IE Cumulative)	Moderate	Remote Code Execution	4021558	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8618						
for x64-based Systems Service Pack 2						

CVE-2017-8619 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8619 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way Microsoft Edge handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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. In addition, an attacker could embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. Finally, the attacker could 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 Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8619						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Edge on Windows 10 for 32-bit Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4025338 (Securit	Critical	Remote Code	4022727	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8619						
on Windows 10 for x64-based Systems	y 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 32-bit Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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-	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8619						
based Systems						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4025342 (Securit	Critical	Remote Code	4022725	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8619						
on Windows 10 Version 1703 for 32-bit Systems	y Update)		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC: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	4025339 (Security Update)	Moderate	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8621 - Microsoft Exchange Open Redirect Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8621 MITRE NVD	**CVE Title:** Microsoft Exchange Open Redirect Vulnerability **Description:** An open redirect vulnerability exists in Microsoft Exchange that could lead to spoofing. To exploit the vulnerability, an attacker could send a link that has a specially crafted URL, and convince the user to click the link. When an authenticated Exchange user clicks the link, the authenticated user's browser session could be redirected to a malicious site that is designed to impersonate a legitimate website. By doing so, the attacker could trick the user and potentially acquire sensitive information, such as the user's credentials. The update addresses the vulnerability by correcting how Exchange handles open redirect requests. **FAQ:** None **Mitigations:** None	Moderate	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Workarounds: None **Revision:** 1.0 2017-07-11T07:00:00 Information Published.		

Affected Software

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

CVE-2017-8621						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Exchange Server 2010 Service Pack 3	4018588 (Security Update)	Moderate	Spoofing	4011326	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2013 Cumulative Update 16	4018588 (Security Update)	Moderate	Spoofing	None	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8621						
Microsoft Exchange Server 2013 Service Pack 1	4018588 (Security Update)	Moderate	Spoofing	4012178	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2016 Cumulative Update 5	4018588 (Security Update)	Moderate	Spoofing	None	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-0170 - Windows Performance Monitor Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-0170 MITRE NVD	**CVE Title:** Windows Performance Monitor Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows Performance Monitor Console when it improperly parses XML input containing a reference to an external entity. An attacker who successfully exploited this vulnerability could read arbitrary files via an XML external entity (XXE) declaration.	Moderate	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit the vulnerability, an attacker could create specially crafted XML data and convince an authenticated user to create a Data Collector Set and import the file. To create a Data Collector Set, the user must be a member of the Performance Log Users or Local Administrators group. The update addresses the vulnerability by modifying the way that the Windows Performance Monitor Console parses XML input. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-0170						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Moderate	Information Disclosure	4022727	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4025338 (Security Update)	Moderate	Information Disclosure	4022727	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Moderate	Information Disclosure	4022714	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Moderate	Information Disclosure	4022714	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-0170						
Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Moderate	Information Disclosure	4022715	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Moderate	Information Disclosure	4022715	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Moderate	Information Disclosure	4022725	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Moderate	Information Disclosure	4022725	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems	4025337 (Security Only)	Moderate	Information Disclosure	4022719	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-0170						
Service Pack 1	4025341 (Monthly Rollup)				CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 7 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Moderate	Information Disclosure	4022719	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Moderate	Information Disclosure	4022726	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Moderate	Information Disclosure	4022726	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-0170						
Windows Server 2008 for 32-bit Systems Service Pack 2	4025397 (Security Update)	Moderate	Information Disclosure	None	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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)	4025397 (Security Update)	Moderate	Information Disclosure	None	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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	4025397 (Security Update)	Moderate	Information Disclosure	None	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-0170						
Windows Server 2008 for x64-based Systems Service Pack 2	4025397 (Security Update)	Moderate	Information Disclosure	None	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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)	4025397 (Security Update)	Moderate	Information Disclosure	None	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems	4025337 (Security Only) 4025341 (Monthly Rollup)	Moderate	Information Disclosure	4022719	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-0170						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Moderate	Information Disclosure	4022719	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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)	4025337 (Security Only) 4025341 (Monthly Rollup)	Moderate	Information Disclosure	4022719	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4025331 (Monthly Rollup) 4025343	Moderate	Information Disclosure	4022724	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-0170						
	(Security Only)				CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4025331 (Monthly Rollup) 4025343 (Security Only)	Moderate	Information Disclosure	4022724	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Moderate	Information Disclosure	4022726	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4025333 (Security Only) 4025336 (Monthly Rollup)	Moderate	Information Disclosure	4022726	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4025339 (Securit	Moderate	Information Disclosure	4022715	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-0170						
	y Update)				CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2016 (Server Core installation)	4025339 (Security Update)	Moderate	Information Disclosure	4022715	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8463 - Windows Explorer Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8463 MITRE NVD	**CVE Title:** Windows Explorer Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists when Windows Explorer improperly handles executable files and shares during rename operations. An attacker who successfully exploited this vulnerability could run arbitrary code in the context of another user. Users not running as administrators would be less affected.	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To exploit this vulnerability, an attacker would first share both a folder and malware named with an executable extension, and then trick the user into thinking that the malware was the folder. The attacker could not force the user to open or browse the share but could use email or instant messages to trick them into doing so. The update addresses the vulnerability by correcting how Windows Explorer handles executable files and shares during rename operations. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8463						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes

CVE-2017-8463						
Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems	4025337 (Security Only)	Critical	Remote Code	4022719	Base: 6.30 Temporal: 6.00 Vector:	Yes

CVE-2017-8463						
Service Pack 1	4025341 (Monthly Rollup)		Execution		CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	
Windows 7 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Critical	Remote Code Execution	4022719	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Critical	Remote Code Execution	4022726	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Critical	Remote Code Execution	4022726	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes

CVE-2017-8463						
Windows RT 8.1	4025336 (Monthly Rollup)	Critical	Remote Code Execution	4022726	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4025497 (Security Update)	Critical	Remote Code Execution	None	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4025497 (Security Update)	Critical	Remote Code Execution	None	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-	4025497 (Securit	Critical	Remote Code	None	Base: 6.30 Temporal: 6.00 Vector:	Yes

CVE-2017-8463						
Based Systems Service Pack 2	y Update)		Execution		CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2	4025497 (Security Update)	Critical	Remote Code Execution	None	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4025497 (Security Update)	Critical	Remote Code Execution	None	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows Server 2008	4025337 (Securit	Critical	Remote Code	4022719	Base: 6.30 Temporal: 6.00	Yes

CVE-2017-8463						
R2 for Itanium-Based Systems Service Pack 1	y Only) 4025341 (Monthly Rollup)		Execution		Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Critical	Remote Code Execution	4022719	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4025337 (Security Only) 4025341 (Monthly Rollup)	Critical	Remote Code Execution	4022719	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes

CVE-2017-8463						
Windows Server 2012	4025331 (Monthly Rollup) 4025343 (Security Only)	Critical	Remote Code Execution	4022724	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4025331 (Monthly Rollup) 4025343 (Security Only)	Critical	Remote Code Execution	4022724	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Critical	Remote Code Execution	4022726	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core	4025333 (Security Only) 4025336	Critical	Remote Code Execution	4022726	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes

CVE-2017-8463						
installation)	(Monthly Rollup)					
Windows Server 2016	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 6.30 Temporal: 6.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:H/RL:O/RC:C	Yes

CVE-2017-8467 - Win32k Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8467	**CVE Title:** Win32k Elevation of Privilege Vulnerability **Description:**	Important	Elevation of Privilege

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8467						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.70 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	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.70 Vector:	Yes

CVE-2017-8467						
					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 1511 for 32-bit Systems	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.70 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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.70 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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.70 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-2017-8467						
Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.70 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	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 7.00 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	Yes
Windows 7 for 32-bit Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.70 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	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.70 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-2017-8467						
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.70 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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.70 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 for 32-bit Systems Service Pack 2	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 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	Unknown

CVE-2017-8467						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 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	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 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 for x64-based Systems Service Pack 2	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 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-2017-8467						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.70 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	4025337 (Security Only) 4025341	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.70 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-2017-8467						
Service Pack 1	(Monthly Rollup)					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.70 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	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4025331 (Monthly Rollup) 4025343	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.70 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-2017-8467						
	(Security Only)					
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.70 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)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.70 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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.70 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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.70 Vector:	Yes

CVE-2017-8467						
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	

CVE-2017-8486 - Win32k Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8486 MITRE NVD	**CVE Title:** Win32k Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in Microsoft Windows when Win32k fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user’s system. To exploit the vulnerability, an attacker could create a special application to run on a target system. The update addresses the vulnerability by correcting how the Win32k 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 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8486						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Information Disclosure	4022727	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes

CVE-2017-8486						
Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Information Disclosure	4022727	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Important	Information Disclosure	4022714	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Information Disclosure	4022714	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Information Disclosure	4022715	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-	4025339 (Securit	Important	Information Disclosure	4022715	Base: 4.70 Temporal: 4.50 Vector:	Yes

CVE-2017-8486						
based Systems	y Update)				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	
Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Information Disclosure	4022725	Base: 4.70 Temporal: 4.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Information Disclosure	4022725	Base: 4.70 Temporal: 4.70 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N	Yes
Windows 7 for 32-bit Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 7 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes

CVE-2017-8486						
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2	4025877 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Unknown

CVE-2017-8486						
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4025877 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4025877 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4025877 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes

CVE-2017-8486						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4025877 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems	4025337 (Security Only) 4025341	Important	Information Disclosure	4022719	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes

CVE-2017-8486						
Service Pack 1	(Monthly Rollup)					
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows Server 2012	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Information Disclosure	4022724	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4025331 (Monthly Rollup) 4025343	Important	Information Disclosure	4022724	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes

CVE-2017-8486						
	(Security Only)					
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows Server 2016	4025339 (Security Update)	Important	Information Disclosure	4022715	Base: 4.70 Temporal: 4.50 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	Yes
Windows Server 2016 (Server Core	4025339 (Security Update)	Important	Information Disclosure	4022715	Base: 4.70 Temporal: 4.50 Vector:	Yes

CVE-2017-8486						
installation)					CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C	

CVE-2017-8495 - Kerberos SNAME Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8495 MITRE NVD	**CVE Title:** Kerberos SNAME Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists in Microsoft Windows when Kerberos fails to prevent tampering with the SNAME field during ticket exchange. An attacker who successfully exploited this vulnerability could use it to bypass Extended Protection for Authentication. To exploit this vulnerability, an attacker would have to be able to launch a man-in-the-middle (MiTM) attack against the traffic passing between a client and the server. The update addresses this vulnerability by adding integrity protection to the SNAME field.	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8495						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Securit	Important	Security	4022727	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8495						
	y Update)		Feature Bypass		CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Security Feature Bypass	4022727	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Important	Security Feature Bypass	4022714	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Security Feature Bypass	4022714	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Security Feature Bypass	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8495						
Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Important	Security Feature Bypass	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Security Feature Bypass	4022725	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Security Feature Bypass	4022725	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Security Feature Bypass	4022719	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-	4025337 (Securit	Important	Security	4022719	Base: 7.50 Temporal: 6.70	Yes

CVE-2017-8495						
based Systems Service Pack 1	y Only) 4025341 (Monthly Rollup)		Feature Bypass		Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Security Feature Bypass	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Security Feature Bypass	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Security Feature Bypass	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008	4022746 (Securit	Important	Security	None	Base: 7.50 Temporal: 6.70	Yes

CVE-2017-8495						
for 32-bit Systems Service Pack 2	y Update)		Feature Bypass		Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4022746 (Security Update)	Important	Security Feature Bypass	None	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4022746 (Security Update)	Important	Security Feature Bypass	3011780	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-	4022746 (Securit	Important	Security	None	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8495						
based Systems Service Pack 2	y Update)		Feature Bypass		CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4022746 (Security Update)	Important	Security Feature Bypass	None	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Security Feature Bypass	4022719	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8495						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Security Feature Bypass	4022719	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Security Feature Bypass	4022719	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Security Feature Bypass	4022724	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8495						
Windows Server 2012 (Server Core installation)	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Security Feature Bypass	4022724	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Security Feature Bypass	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Security Feature Bypass	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4025339 (Security Update)	Important	Security Feature Bypass	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8495						
Windows Server 2016 (Server Core installation)	4025339 (Security Update)	Important	Security Feature Bypass	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8501 - Microsoft Office Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8501 MITRE NVD	**CVE Title:** Microsoft Office Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. Note that the Preview Pane is not an attack vector for this vulnerability. The security update addresses the vulnerability by correcting how Office handles objects in memory. **FAQ:** None **Mitigations:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8501						
Product	**KB Article**	**Severity**	**Impact**	**Supersedence**	**CVSS Score Set**	**Restart Required**
Excel Services on Microsoft SharePoint Server 2010 Service Pack 2	3191902 (Security Update)	Important	Remote Code Execution	3191840	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2007 Service Pack 3	3191894 (Security Update)	Important	Remote Code Execution	3191827	Base: N/A Temporal:	Maybe

CVE-2017-8501						
					N/A Vector: N/A	
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	3191907 (Security Update)	Important	Remote Code Execution	3191847	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	3191907 (Security Update)	Important	Remote Code Execution	3191847	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 RT Service Pack 1	3213537 (Security Update)	Important	Remote Code Execution	3172542	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	3213537 (Security Update)	Important	Remote Code Execution	3172542	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	3213537 (Security Update)	Important	Remote Code Execution	3172542	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8501						
Microsoft Excel 2016 (32-bit edition)	3203477 (Security Update)	Important	Remote Code Execution	3178673	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	3203477 (Security Update)	Important	Remote Code Execution	3178673	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel Viewer 2007 Service Pack 3	3191833 (Security Update)	Important	Remote Code Execution	3178680	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office 2016 for Mac	3212224 (Security Update)	Important	Remote Code Execution	3212223	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office Compatibility Pack Service Pack 3	3191897 (Security Update)	Important	Remote Code Execution	3191830	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Office for Mac 2011	3212224 (Security Update)	Important	Remote Code Execution	3212223	Base: N/A Temporal:	Maybe

CVE-2017-8501						
					N/A Vector: N/A	
Microsoft Office Online Server 2016	3213657 (Security Update)	Important	Remote Code Execution	3203485	Base: N/A Temporal: N/A Vector: N/A	Unknown
Microsoft SharePoint Enterprise Server 2013	3213559 (Security Update)	Important	Remote Code Execution	3203390	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8502 - Microsoft Office Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8502 MITRE NVD	**CVE Title:** Microsoft Office Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. Exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Office software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) that contains a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. Note that the Preview Pane is not an attack vector for this vulnerability. The security update addresses the vulnerability by correcting how Office handles objects in memory.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8502						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Excel 2010 Service Pack 2 (32-bit editions)	3191907 (Security Update)	Important	Remote Code Execution	3191847	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8502						
Microsoft Excel 2010 Service Pack 2 (64-bit editions)	3191907 (Security Update)	Important	Remote Code Execution	3191847	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 RT Service Pack 1	3213537 (Security Update)	Important	Remote Code Execution	3172542	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (32-bit editions)	3213537 (Security Update)	Important	Remote Code Execution	3172542	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2013 Service Pack 1 (64-bit editions)	3213537 (Security Update)	Important	Remote Code Execution	3172542	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (32-bit edition)	3203477 (Security Update)	Important	Remote Code Execution	3178673	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Excel 2016 (64-bit edition)	3203477 (Security Update)	Important	Remote Code Execution	3178673	Base: N/A Temporal:	Maybe

CVE-2017-8502						
					N/A Vector: N/A	

CVE-2017-8556 - Microsoft Graphics Component Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8556 MITRE NVD	**CVE Title:** Microsoft Graphics Component Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows when the Microsoft Graphics Component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses this vulnerability by correcting how the Microsoft Graphics Component handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8556						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8556						
Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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 32-bit Systems	4025337 (Security Only)	Important	Elevation of	4022719	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8556						
Service Pack 1	4025341 (Monthly Rollup)		Privilege		CVSS: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 7 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8556						
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Unknown
Windows Server 2008 for Itanium-	4025877 (Securit	Important	Elevation of	None	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8556						
Based Systems Service Pack 2	y Update)		Privilege		CVSS: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 x64-based Systems Service Pack 2	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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)	4025877 (Security Update)	Important	Elevation of Privilege	None	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025337 (Securit	Important	Elevation of	4022719	Base: 7.00 Temporal: 6.30	Yes

CVE-2017-8556						
R2 for Itanium-Based Systems Service Pack 1	y Only) 4025341 (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 x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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)	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8556						
Windows Server 2012	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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)	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025333 (Security Only) 4025336	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8556						
installation)	(Monthly Rollup)					
Windows Server 2016	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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)	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8557 - Windows System Information Console Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8557 MITRE NVD	**CVE Title:** Windows System Information Console Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists in the Windows System Information Console when it improperly parses XML input containing a reference to an external entity. An attacker who successfully exploited this vulnerability could read arbitrary files via an XML external entity (XXE) declaration. To exploit the vulnerability, an attacker could create a file containing specially crafted XML content and convince an authenticated user to open the file. The update addresses the vulnerability by modifying the way that the Windows System Information Console parses XML input. **FAQ:** None **Mitigations:**	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8557						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Information Disclosure	4022727	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8557						
Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Information Disclosure	4022727	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Important	Information Disclosure	4022714	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Information Disclosure	4022714	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Information Disclosure	4022715	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607 for x64-	4025339 (Securit	Important	Information Disclosure	4022715	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8557						
based Systems	y Update)				CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Information Disclosure	4022725	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Information Disclosure	4022725	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 7 for x64-based Systems	4025337 (Security Only) 4025341	Important	Information Disclosure	4022719	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8557						
Service Pack 1	(Monthly Rollup)					
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems	4025398 (Security Update)	Important	Information Disclosure	None	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8557						
Service Pack 2					CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4025398 (Security Update)	Important	Information Disclosure	None	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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	4025398 (Security Update)	Important	Information Disclosure	None	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems	4025398 (Security Update)	Important	Information Disclosure	None	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8557						
Service Pack 2						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4025398 (Security Update)	Important	Information Disclosure	None	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-	4025337 (Security Only)	Important	Information Disclosure	4022719	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8557						
based Systems Service Pack 1	4025341 (Monthly Rollup)				CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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)	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Information Disclosure	4022724	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core	4025331 (Monthly Rollup)	Important	Information Disclosure	4022724	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8557						
installation)	4025343 (Security Only)				CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016	4025339 (Security Update)	Important	Information Disclosure	4022715	Base: 5.50 Temporal: 5.00 Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core	4025339 (Securit	Important	Information Disclosure	4022715	Base: 5.50 Temporal: 5.00 Vector:	Yes

CVE-2017-8557						
installation)	y Update)				CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	

CVE-2017-8560 - Microsoft Exchange Cross-Site Scripting Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8560 MITRE NVD	**CVE Title:** Microsoft Exchange Cross-Site Scripting Vulnerability **Description:** An elevation of privilege vulnerability exists when Microsoft Exchange Outlook Web Access (OWA) fails to properly handle web requests. An attacker who successfully exploited this vulnerability could perform script/content injection attacks 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. Alternatively, an attacker could use a chat client to social engineer a user into clicking the malicious link. The security update addresses the vulnerability by correcting how Microsoft Exchange validates web requests.	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Note: In order to exploit this vulnerability, a user must click a maliciously crafted link from an attacker. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8560						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required

CVE-2017-8560						
Microsoft Exchange Server 2013 Cumulative Update 16	4018588 (Security Update)	Important	Elevation of Privilege	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2013 Service Pack 1	4018588 (Security Update)	Important	Elevation of Privilege	4012178	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2016 Cumulative Update 5	4018588 (Security Update)	Important	Elevation of Privilege	None	Base: N/A Temporal: N/A Vector: N/A	Maybe

CVE-2017-8559 - Microsoft Exchange Cross-Site Scripting Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8559	**CVE Title:** Microsoft Exchange Cross-Site Scripting Vulnerability **Description:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	An elevation of privilege vulnerability exists when Microsoft Exchange Outlook Web Access (OWA) fails to properly handle web requests. An attacker who successfully exploited this vulnerability could perform script/content injection attacks 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. Alternatively, an attacker could use a chat client to social engineer a user into clicking the malicious link. The security update addresses the vulnerability by correcting how Microsoft Exchange validates web requests. Note: In order to exploit this vulnerability, a user must click a maliciously crafted link from an attacker. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8559						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Exchange Server 2013 Cumulative Update 16	4018588 (Security Update)	Important	Elevation of Privilege	None	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2013 Service Pack 1	4018588 (Security Update)	Important	Elevation of Privilege	4012178	Base: N/A Temporal: N/A Vector: N/A	Maybe
Microsoft Exchange Server 2016 Cumulative Update 5	4018588 (Security Update)	Important	Elevation of Privilege	None	Base: N/A Temporal:	Maybe

CVE-2017-8559						
					N/A Vector: N/A	

CVE-2017-8561 - Windows Kernel Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8561 MITRE NVD	**CVE Title:** Windows Kernel Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses the vulnerability by ensuring the Windows Kernel properly handles objects in memory. **FAQ:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8561						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8561						
Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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-	4025339 (Securit	Important	Elevation of	4022715	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8561						
based Systems	y Update)		Privilege		CVSS: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 32-bit Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025333 (Security Only) 4025336	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8561						
	(Monthly Rollup)					
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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)	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025333 (Security Only) 4025336	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8561						
	(Monthly Rollup)				CVSS: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)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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)	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8562 - Windows ALPC Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8562 MITRE NVD	**CVE Title:** Windows ALPC Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC). An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would 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 over an affected system. The update addresses the vulnerability by correcting how Windows handles calls to ALPC. **FAQ:** None	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Mitigations: None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8562						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8562						
Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Elevation of Privilege	4022727	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025344 (Security Update)	Important	Elevation of Privilege	4022714	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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-	4025339 (Securit	Important	Elevation of	4022715	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8562						
based Systems	y Update)		Privilege		CVSS: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 32-bit Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025333 (Security Only) 4025336	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8562						
	(Monthly Rollup)					
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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)	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025333 (Security Only) 4025336	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8562						
	(Monthly Rollup)				CVSS: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)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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)	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8563 - Windows Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8563 MITRE NVD	**CVE Title:** Windows Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Microsoft Windows when Kerberos falls back to NT LAN Manager (NTLM) Authentication Protocol as the default authentication protocol. In a remote attack scenario, an attacker could exploit this vulnerability by running a specially crafted application to send malicious traffic to a domain controller. An attacker who successfully exploited this vulnerability could run processes in an elevated context. The update addresses this vulnerability by incorporating enhancements to authentication protocols designed to mitigate authentication attacks. It revolves around the concept of channel binding information. **FAQ:** **In addition to installing the updates for CVE-2017-8563 are there any further steps I need to carry out to be protected from this CVE?**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Yes. To make LDAP authentication over SSL/TLS more secure, administrators need to create a LdapEnforceChannelBinding registry setting on a Domain Controller. For more information about setting this registry key, see Microsoft Knowledge Base article 4034879. **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8563						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 for 32-bit Systems	4025338 (Securit	Important	Elevation of	4022727	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8563						
	y Update)		Privileg e		CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/R C:C	
Windows 10 for x64-based Systems	4025338 (Securit y Update)	Importan t	Elevatio n of Privileg e	4022727	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/R C:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4025344 (Securit y Update)	Importan t	Elevatio n of Privileg e	4022714	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/R C:C	Yes
Windows 10 Version 1511 for x64-based Systems	4025344 (Securit y Update)	Importan t	Elevatio n of Privileg e	4022714	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/R C:C	Yes
Windows 10 Version 1607 for 32-bit Systems	4025339 (Securit y Update)	Importan t	Elevatio n of Privileg e	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/R C:C	Yes

CVE-2017-8563						
Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for x64-	4025337 (Securit	Important	Elevation of	4022719	Base: 7.50 Temporal: 6.70	Yes

CVE-2017-8563						
based Systems Service Pack 1	y Only) 4025341 (Monthly Rollup)		Privilege		Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008	4025409 (Securit	Important	Elevation of	3184471	Base: 7.50 Temporal: 6.70	Yes

CVE-2017-8563						
for 32-bit Systems Service Pack 2	y Update)		Privilege		Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4025409 (Security Update)	Important	Elevation of Privilege	3184471	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for Itanium-Based Systems Service Pack 2	4025409 (Security Update)	Important	Elevation of Privilege	3184471	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-	4025409 (Securit	Important	Elevation of	3184471	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8563						
based Systems Service Pack 2	y Update)		Privilege		CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4025409 (Security Update)	Important	Elevation of Privilege	3184471	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8563						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Elevation of Privilege	4022719	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8563						
Windows Server 2012 (Server Core installation)	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Elevation of Privilege	4022724	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2 (Server Core installation)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Elevation of Privilege	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8563						
Windows Server 2016 (Server Core installation)	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8564 - Windows Kernel Information Disclosure Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8564 MITRE NVD	**CVE Title:** Windows Kernel Information Disclosure Vulnerability **Description:** An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, allowing an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (KASLR) bypass. An attacker who successfully exploited this vulnerability could retrieve the base address of the kernel driver from a compromised process. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.	Important	Information Disclosure

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The security update addresses the vulnerability by correcting how the Windows kernel handles memory addresses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8564						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required

CVE-2017-8564						
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Information Disclosure	4022727	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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	4025338 (Security Update)	Important	Information Disclosure	4022727	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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	4025344 (Security Update)	Important	Information Disclosure	4022714	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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	4025344 (Security Update)	Important	Information Disclosure	4022714	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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	4025339 (Securit	Important	Information Disclosure	4022715	Base: 4.70 Temporal: 4.20 Vector:	Yes

CVE-2017-8564						
for 32-bit Systems	y Update)				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Important	Information Disclosure	4022715	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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	4025342 (Security Update)	Important	Information Disclosure	4022725	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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	4025342 (Security Update)	Important	Information Disclosure	4022725	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/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 32-bit Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8564						
Windows 7 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/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	4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8564						
Windows Server 2008 for 32-bit Systems Service Pack 2	4022748 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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)	4022748 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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	4022748 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8564						
Windows Server 2008 for x64-based Systems Service Pack 2	4022748 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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)	4022748 (Security Update)	Important	Information Disclosure	None	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8564						
Service Pack 1						
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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)	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Information Disclosure	4022719	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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	4025331 (Monthly Rollup) 4025343	Important	Information Disclosure	4022724	Base: 4.70 Temporal: 4.20 Vector:	Yes

CVE-2017-8564						
	(Security Only)				CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	
Windows Server 2012 (Server Core installation)	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Information Disclosure	4022724	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Information Disclosure	4022726	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV: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	4025339 (Securit	Important	Information Disclosure	4022715	Base: 4.70 Temporal: 4.20 Vector:	Yes

CVE-2017-8564						
	y 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)	4025339 (Security Update)	Important	Information Disclosure	4022715	Base: 4.70 Temporal: 4.20 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8565 - Windows PowerShell Remote Code Execution Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8565 MITRE NVD	**CVE Title:** Windows PowerShell Remote Code Execution Vulnerability **Description:** A remote code execution vulnerability exists in PowerShell when PSObject wraps a CIM Instance. An attacker who successfully exploited this vulnerability could execute malicious code on a vulnerable system. In an attack scenario, an attacker could execute malicious code in a PowerShell remote session.	Important	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	The update addresses the vulnerability by correcting how PowerShell deserializes user supplied scripts. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8565						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required

CVE-2017-8565						
Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Remote Code Execution	4022727	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Remote Code Execution	4022727	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Important	Remote Code Execution	4022714	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Remote Code Execution	4022714	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1607	4025339 (Securit	Important	Remote Code	4022715	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8565						
for 32-bit Systems	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Important	Remote Code Execution	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Remote Code Execution	4022725	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Remote Code Execution	4022725	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 7 for 32-bit Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Remote Code Execution	4022719	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8565						
Windows 7 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Remote Code Execution	4022719	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for 32-bit systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Remote Code Execution	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 8.1 for x64-based systems	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Remote Code Execution	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows RT 8.1	4025336 (Monthly Rollup)	Important	Remote Code Execution	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8565						
Windows Server 2008 for 32-bit Systems Service Pack 2	4025872 (Security Update)	Important	Remote Code Execution	None	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	4025872 (Security Update)	Important	Remote Code Execution	None	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 for x64-based Systems Service Pack 2	4025872 (Security Update)	Important	Remote Code Execution	None	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8565						
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4025872 (Security Update)	Important	Remote Code Execution	None	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Remote Code Execution	4022719	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2008 R2 for x64-based Systems Service Pack	4025337 (Security Only) 4025341 (Monthly Rollup)	Important	Remote Code Execution	4022719	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8565						
1 (Server Core installation)						
Windows Server 2012	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Remote Code Execution	4022724	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 (Server Core installation)	4025331 (Monthly Rollup) 4025343 (Security Only)	Important	Remote Code Execution	4022724	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2012 R2	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Remote Code Execution	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8565						
Windows Server 2012 R2 (Server Core installation)	4025333 (Security Only) 4025336 (Monthly Rollup)	Important	Remote Code Execution	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016	4025339 (Security Update)	Important	Remote Code Execution	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows Server 2016 (Server Core installation)	4025339 (Security Update)	Important	Remote Code Execution	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8566 - Windows IME Elevation of Privilege Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8566 MITRE NVD	**CVE Title:** Windows IME Elevation of Privilege Vulnerability **Description:** An elevation of privilege vulnerability exists in Windows Input Method Editor (IME) when IME improperly handles parameters in a method of a DCOM class. The DCOM server is a Windows component installed regardless of which languages/IMEs are enabled. An attacker can instantiate the DCOM class and exploit the system even if IME is not enabled. To exploit this vulnerability, a locally authenticated attacker could run a specially crafted application. The security update addresses this vulnerability by correcting how Windows IME handles parameters in a method of a DCOM class. **FAQ:** None **Mitigations:**	Important	Elevation of Privilege

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8566						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8566						
Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Elevation of Privilege	4022725	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Security Update)	Important	Elevation of Privilege	4022715	Base: 7.00 Temporal: 6.30 Vector: CVSS:3.0/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	4025339 (Securit	Important	Elevation of	4022715	Base: 7.00 Temporal: 6.30 Vector:	Yes

CVE-2017-8566						
installation)	y Update)		Privilege		CVSS: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-2017-8598 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8598 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way Microsoft Edge handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	and then convince a user to view the website. In addition, an attacker could embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. Finally, the attacker could 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 Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8598						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8598						
x64-based Systems						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8598						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4025339 (Security Update)	Moderate	Remote Code Execution	4022715	Base: 3.10 Temporal: 2.80 Vector:	Yes

CVE-2017-8598						
Server 2016					CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	

CVE-2017-8599 - Microsoft Edge Security Feature Bypass Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8599 MITRE NVD	**CVE Title:** Microsoft Edge Security Feature Bypass Vulnerability **Description:** A security feature bypass vulnerability exists when Microsoft Edge fails to correctly apply Same Origin Policy for HTML elements present in other browser windows. An attacker could use this vulnerability to trick a user into loading a page with malicious content. To exploit this vulnerability, an attacker would need to trick a user into loading a page or visiting a website. The page could also be injected into a compromised website or ad network. The update addresses the vulnerability by correcting the Same Origin Policy check for scripts attempting to manipulate HTML elements in other browser windows.	Important	Security Feature Bypass

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8599						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Edge on	4025338 (Securit	Important	Security	4022727	Base: 6.50 Temporal: 5.90 Vector:	Yes

CVE-2017-8599						
Windows 10 for 32-bit Systems	y Update)		Feature Bypass		CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Security Feature Bypass	4022727	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Important	Security Feature Bypass	4022714	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4025344 (Securit	Important	Security	4022714	Base: 6.50 Temporal: 5.90	Yes

CVE-2017-8599						
on Windows 10 Version 1511 for x64-based Systems	y Update)		Feature Bypass		Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Security Feature Bypass	4022715	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4025339 (Security Update)	Important	Security Feature Bypass	4022715	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8599						
1607 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Security Feature Bypass	4022725	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Important	Security Feature Bypass	4022725	Base: 6.50 Temporal: 5.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8599						
Microsoft Edge on Windows Server 2016	4025339 (Security Update)	Low	Security Feature Bypass	4022715	Base: 4.50 Temporal: 4.10 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8601 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8601 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way that the Chakra JavaScript engine renders when handling 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. 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. An attacker could also embed an	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the Edge 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. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. The update addresses the vulnerability by modifying how the Chakra JavaScript scripting engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	Revision: 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8601						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Edge on Windows 10 for 32-bit Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4025338 (Securit	Critical	Remote Code	4022727	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8601						
on Windows 10 for x64-based Systems	y 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 32-bit Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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-	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8601						
based Systems						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4025342 (Securit	Critical	Remote Code	4022725	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8601						
on Windows 10 Version 1703 for 32-bit Systems	y Update)		Execution		Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC: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	4025339 (Security Update)	Moderate	Remote Code Execution	4022715	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8602 - Microsoft Browser Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8602 MITRE NVD	**CVE Title:** Microsoft Browser Spoofing Vulnerability **Description:** A spoofing vulnerability exists when an affected Microsoft browser does not properly parse HTTP content. An attacker who successfully exploited this vulnerability could trick a user by redirecting the user to a specially crafted website. The specially crafted website could either spoof content or serve as a pivot to chain an attack with other vulnerabilities in web services. To exploit the vulnerability, the user must click a specially crafted URL. In an email attack scenario, an attacker could send an email message containing the specially crafted URL to the user in an attempt to convince the user to click it. In a web-based attack scenario, an attacker could host a specially crafted website designed to appear as a legitimate website to the user. However, the attacker would have no way to force the user to visit the specially crafted website. The attacker would have to convince the user to visit the specially	Important	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	crafted website, typically via an enticement in email or instant message, and then convince the user to interact with content on the website. The security update addresses the vulnerability by correcting how Microsoft browsers parse HTTP responses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8602						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Internet Explorer 11 on Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Spoofing	4022727	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Spoofing	4022727	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10	4025344 (Security Update)	Important	Spoofing	4022714	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes

CVE-2017-8602						
Version 1511 for 32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Spoofing	4022714	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Spoofing	4022715	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes

CVE-2017-8602						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Important	Spoofing	4022715	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Spoofing	4022725	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4025342 (Security Update)	Important	Spoofing	4022725	Base: 4.30 Temporal: 4.00 Vector:	Yes

CVE-2017-8602						
10 Version 1703 for x64-based Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4025341 (Monthly Rollup) 4025252 (IE Cumulative)	Important	Spoofing	4022719 4021558	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for x64-based Systems	4025341 (Monthly Rollup) 4025252 (IE Cumulative)	Important	Spoofing	4022719 4021558	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes

CVE-2017-8602						
Service Pack 1						
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Important	Spoofing	4022726 4021558	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Important	Spoofing	4022726 4021558	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Internet Explorer 11 on Windows RT 8.1	4025336 (Monthly Rollup)	Important	Spoofing	4022726	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes

CVE-2017-8602						
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025341 (Monthly Rollup) 4025252 (IE Cumulative)	Low	Spoofing	4022719 4021558	Base: 2.40 Temporal: 2.30 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Low	Spoofing	4022726 4021558	Base: 2.40 Temporal: 2.30 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4025339 (Security Update)	Low	Spoofing	4022715	Base: 2.40 Temporal: 2.30 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes

CVE-2017-8602						
Server 2016						
Microsoft Edge on Windows 10 for 32-bit Systems	4025338 (Security Update)	Important	Spoofing	4022727	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4025338 (Security Update)	Important	Spoofing	4022727	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4025344 (Security Update)	Important	Spoofing	4022714	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes

CVE-2017-8602						
1511 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Important	Spoofing	4022714	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Important	Spoofing	4022715	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes

CVE-2017-8602						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Important	Spoofing	4022715	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Important	Spoofing	4022725	Base: 4.30 Temporal: 4.00 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes
Microsoft Edge on Windows	4025342 (Security Update)	Important	Spoofing	4022725	Base: 4.30 Temporal: 4.00 Vector:	Yes

CVE-2017-8602						
10 Version 1703 for x64-based Systems					CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	
Microsoft Edge on Windows Server 2016	4025339 (Security Update)	Low	Spoofing	4022715	Base: 2.40 Temporal: 2.30 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N/E:F/RL:O/RC:C	Yes

CVE-2017-8603 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8603	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists in the way Microsoft Edge handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. In addition, an attacker could embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. Finally, the attacker could 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 Microsoft Edge handles objects in memory.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8603						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Edge on	4025344 (Securit	Critical	Remote Code	4022714	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8603						
Windows 10 Version 1511 for 32-bit Systems	y Update)		Execution		CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8603						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge	4025342 (Securit	Critical	Remote Code	4022725	Base: 4.20 Temporal: 3.80	Yes

CVE-2017-8603						
on Windows 10 Version 1703 for x64-based Systems	y 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 Server 2016	4025339 (Security Update)	Moderate	Remote Code Execution	4022715	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8604 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8604 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way Microsoft Edge handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. In addition, an attacker could embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. Finally, the attacker could take advantage of compromised websites, and websites that	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8604						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8604						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8604						
10 Version 1703 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 1703 for x64-based Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC: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	4025339 (Security Update)	Moderate	Remote Code Execution	4022715	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8605 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8605 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way Microsoft Edge handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge and then convince a user to view the website. In addition, an attacker could embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. Finally, the attacker could take advantage of compromised websites, and websites that	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8605						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Edge on Windows 10 for 32-bit Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/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	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8605						
Version 1511 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8605						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8605						
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 Server 2016	4025339 (Security Update)	Moderate	Remote Code Execution	4022715	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8606 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8606	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Moderate	Remote Code Execution

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	FAQ: None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8606						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Internet Explorer 10 on	4025331 (Monthly Rollup)	Moderate	Remote Code	4022724 4021558	Base: 3.10 Temporal: 2.80 Vector:	Yes

CVE-2017-8606						
Windows Server 2012	4025252 (IE Cumulative)		Execution		CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 for 32-bit Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-based Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8606						
10 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	
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8606						
32-bit Systems						
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8606						
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1	4025252 (IE Cumulative)	Critical	Remote Code Execution	4021558	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4025252 (IE Cumulative)	Critical	Remote Code Execution	4021558	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8606						
7 for x64-based Systems Service Pack 1					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Critical	Remote Code Execution	4022726 4021558	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for x64-based systems	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Critical	Remote Code Execution	4022726 4021558	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8606						
Internet Explorer 11 on Windows RT 8.1	4025336 (Monthly Rollup)	Critical	Remote Code Execution	4022726	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025252 (IE Cumulative)	Moderate	Remote Code Execution	4021558	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2012 R2	4025252 (IE Cumulative)	Moderate	Remote Code Execution	4021558	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8606						
Internet Explorer 11 on Windows Server 2016	4025339 (Security Update)	Moderate	Remote Code Execution	4022715	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4025252 (IE Cumulative)	Moderate	Remote Code Execution	4021558	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-	4025252 (IE Cumulative)	Moderate	Remote Code Execution	4021558	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8606						
based Systems Service Pack 2						
Microsoft Edge on Windows 10 for 32-bit Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/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	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8606						
10 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 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8606						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8606						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC: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	4025339 (Security Update)	Moderate	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8607 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8607 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way JavaScript engines render when handling objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website designed to exploit the vulnerability through a Microsoft browser and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8607						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Internet Explorer 10 on Windows Server 2012	4025331 (Monthly Rollup) 4025252 (IE Cumulative)	Moderate	Remote Code Execution	4022724 4021558	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for 32-bit Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 for x64-	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8607						
based Systems						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8607						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8607						
10 Version 1703 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	
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 7 for 32-bit Systems	4025252 (IE Cumulative)	Critical	Remote Code Execution	4021558	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8607						
Service Pack 1						
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1	4025252 (IE Cumulative)	Critical	Remote Code Execution	4021558	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 8.1 for 32-bit systems	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Critical	Remote Code Execution	4022726 4021558	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4025336 (Monthly Rollup) 4025252	Critical	Remote Code Execution	4022726 4021558	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8607						
8.1 for x64-based systems	(IE Cumulative)				CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows RT 8.1	4025336 (Monthly Rollup)	Critical	Remote Code Execution	4022726	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1	4025252 (IE Cumulative)	Moderate	Remote Code Execution	4021558	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on	4025336 (Monthly Rollup)	Moderate	Remote Code	4022726 4021558	Base: 3.10 Temporal: 2.80 Vector:	Yes

CVE-2017-8607						
Windows Server 2012 R2	4025252 (IE Cumulative)		Execution		CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows Server 2016	4025339 (Security Update)	Moderate	Remote Code Execution	4022715	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2	4025252 (IE Cumulative)	Moderate	Remote Code Execution	4021558	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on	4025252 (IE	Moderate	Remote Code	4021558	Base: 3.10 Temporal: 2.80 Vector:	Yes

CVE-2017-8607						
Windows Server 2008 for x64-based Systems Service Pack 2	Cumulative)		Execution		CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	
Microsoft Edge on Windows 10 for 32-bit Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/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	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8607						
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8607						
10 Version 1607 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 1607 for x64-based Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8607						
32-bit Systems						
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC: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	4025339 (Security Update)	Moderate	Remote Code Execution	4022715	Base: 3.10 Temporal: 2.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8608 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8608 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way JavaScript engines render when handling objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website designed to exploit the vulnerability through a Microsoft browser and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability. The security update addresses the vulnerability by modifying how Microsoft browser JavaScript scripting engines handle objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8608						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Internet Explorer 10 on Windows Server 2012	4025331 (Monthly Rollup) 4025252 (IE Cumulative)	Moderate	Remote Code Execution	4022724 4021558	Base: 6.40 Temporal: 5.80 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 for 32-bit Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/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-	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8608						
based Systems						
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8608						
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/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	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 11 on Windows	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 7.50 Temporal: 6.70 Vector:	Yes

CVE-2017-8608						
10 Version 1703 for 32-bit Systems					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/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 32-bit systems	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Critical	Remote Code Execution	4022726 4021558	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8608						
Internet Explorer 11 on Windows 8.1 for x64-based systems	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Critical	Remote Code Execution	4022726 4021558	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/PR:N/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	4025336 (Monthly Rollup)	Critical	Remote Code Execution	4022726	Base: 7.50 Temporal: 6.70 Vector: CVSS:3.0/AV:N/AC:H/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	4025336 (Monthly Rollup) 4025252 (IE Cumulative)	Moderate	Remote Code Execution	4022726 4021558	Base: 6.40 Temporal: 5.80 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	4025339 (Security Update)	Moderate	Remote Code	4022715	Base: 6.40 Temporal: 5.80 Vector:	Yes

CVE-2017-8608						
Windows Server 2016			Execution		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 32-bit Systems Service Pack 2	4025252 (IE Cumulative)	Moderate	Remote Code Execution	4021558	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes
Internet Explorer 9 on Windows Server 2008 for x64-based Systems	4025252 (IE Cumulative)	Moderate	Remote Code Execution	4021558	Base: 6.40 Temporal: 5.80 Vector: CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	Yes

CVE-2017-8608						
Service Pack 2						
Microsoft Edge on Windows 10 for 32-bit Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/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	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8608						
1511 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8608						
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8608						
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 Server 2016	4025339 (Security Update)	Moderate	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8609 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8609	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:**	Moderate	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
MITRE NVD	A remote code execution vulnerability exists in the way that the Scripting Engine renders when handling objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer or Microsoft Edge 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 scripting 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 vulnerabilities. The security update addresses the vulnerability by modifying how the Scripting Engine handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:**		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8609						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Edge on Windows 10 for 32-bit Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8609						
Microsoft Edge on Windows 10 for x64-based Systems	4025338 (Security Update)	Critical	Remote Code Execution	4022727	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4025344 (Security Update)	Critical	Remote Code Execution	4022714	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8609						
1511 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025339 (Security Update)	Critical	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8609						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4025339 (Security Update)	Moderate	Remote Code Execution	4022715	Base: 4.20 Temporal: 3.80 Vector:	Yes

CVE-2017-8609						
Server 2016					CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	

CVE-2017-8610 - Scripting Engine Memory Corruption Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8610 MITRE NVD	**CVE Title:** Scripting Engine Memory Corruption Vulnerability **Description:** A remote code execution vulnerability exists in the way Microsoft Edge handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	and then convince a user to view the website. In addition, an attacker could embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the browser rendering engine. Finally, the attacker could 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 Microsoft Edge handles objects in memory. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8610						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR: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	4025342 (Security Update)	Critical	Remote Code Execution	4022725	Base: 4.20 Temporal: 3.80 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8610						
x64-based Systems						

CVE-2017-8611 - Microsoft Edge Spoofing Vulnerability

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
CVE-2017-8611 MITRE NVD	**CVE Title:** Microsoft Edge Spoofing Vulnerability **Description:** A spoofing vulnerability exists when Microsoft Edge does not properly parse HTTP content. An attacker who successfully exploited this vulnerability could trick a user by redirecting the user to a specially crafted website. The specially crafted website could either spoof content or serve as a pivot to chain an attack with other vulnerabilities in web services. To exploit the vulnerability, the user must click a specially crafted URL. In an email attack scenario, an attacker could send an email message containing the specially crafted URL to the user in an attempt to convince the user to click it.	Moderate	Spoofing

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	In a web-based attack scenario, an attacker could host a specially crafted website designed to appear as a legitimate website to the user. However, the attacker would have no way to force the user to visit the specially crafted website. The attacker would have to convince the user to visit the specially crafted website, typically by way of enticement in an email or instant message, and then convince the user to interact with content on the website. The update addresses the vulnerability by correcting how Microsoft Edge parses HTTP responses. **FAQ:** None **Mitigations:** None **Workarounds:** None **Revision:** 1.0 2017-07-11T07:00:00 Information published.		

Affected Software

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

CVE-2017-8611						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Microsoft Edge on Windows 10 for 32-bit Systems	4025338 (Security Update)	Moderate	Spoofing	4022727	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 for x64-based Systems	4025338 (Security Update)	Moderate	Spoofing	4022727	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version	4025344 (Security Update)	Moderate	Spoofing	4022714	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8611						
1511 for 32-bit Systems						
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems	4025344 (Security Update)	Moderate	Spoofing	4022714	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems	4025339 (Security Update)	Moderate	Spoofing	4022715	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10	4025339 (Security Update)	Moderate	Spoofing	4022715	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes

CVE-2017-8611						
Version 1607 for x64-based Systems						
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems	4025342 (Security Update)	Moderate	Spoofing	4022725	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems	4025342 (Security Update)	Moderate	Spoofing	4022725	Base: 4.30 Temporal: 3.90 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	Yes
Microsoft Edge on Windows	4025339 (Security Update)	Low	Spoofing	4022715	Base: 4.30 Temporal: 3.90	Yes

CVE-2017-8611						
Server 2016					Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C	

ADV170009 - July Flash Security Update

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
ADV170009 MITRE NVD	**CVE Title:** July Flash Security Update **Description:** This security update addresses the following vulnerabilities, which are described in Adobe Security Bulletin APSB17-21: CVE-2017-3099, CVE-2017-3080, CVE-2017-3100 **FAQ:** **How could an attacker exploit these vulnerabilities?** In a web-based attack scenario where the user is using Internet Explorer for the desktop, an attacker could host a specially crafted website that is designed to exploit any of these vulnerabilities through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised	Critical	Remote Code Execution

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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.		

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	1. Paste the following into a text file and save it with the .reg file extension. Copy Windows Registry Editor Version 5.00 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] "Compatibility Flags"=dword:00000400 [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\ActiveX Compatibility\{D27CDB6E-AE6D-11CF-96B8-444553540000}] "Compatibility Flags"=dword:00000400 2. Double-click the .reg file to apply it to an individual system. You can also apply this workaround across domains by using Group Policy. For more information about Group Policy, see the TechNet article, Group Policy collection.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To disable Adobe Flash Player in Internet Explorer through Group Policy, perform the following steps: **Note** This workaround does not prevent Flash from being invoked from other applications, such as Microsoft Office 2007 or Microsoft Office 2010. 1. Open the Group Policy Management Console and configure the console to work with the appropriate Group Policy object, such as local machine, OU, or domain GPO. 2. Navigate to the following node: **Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Add-on Management** 3. Double-click **Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects.** 4. Change the setting to **Enabled.** 5. Click **Apply** and then click **OK** to return to the Group Policy Management Console.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	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.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	To disable Adobe Flash Player in Office 2010 only, set the kill bit for the ActiveX control for Adobe Flash Player in the registry using the following steps: 1. Create a text file named Disable_Flash.reg with the following contents: Copy Windows Registry Editor Version 5.00 [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.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	• **Prevent ActiveX controls from running in Office 2007 and Office 2010** To disable all ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, including Adobe Flash Player in Internet Explorer, perform the following steps: 1. Click **File**, click **Options**, click **Trust Center**, and then click **Trust Center Settings**. 2. Click **ActiveX Settings** in the left-hand pane, and then select **Disable all controls without notifications**. 3. Click **OK** to save your settings. **Impact of workaround.** Office documents that use embedded ActiveX controls may not display as intended. **How to undo the workaround.** To re-enable ActiveX controls in Microsoft Office 2007 and Microsoft Office 2010, perform the following steps:		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	4. Click **File**, click **Options**, click **Trust Center**, and then click **Trust Center Settings**. 5. Click **ActiveX Settings** in the left-hand pane, and then deselect **Disable all controls without notifications**. 6. Click **OK** to save your settings. • **Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones** You can help protect against exploitation of these vulnerabilities by changing your settings for the Internet security zone to block ActiveX controls and Active Scripting. You can do this by setting your browser security to High. To raise the browsing security level in Internet Explorer, perform the following steps: 1. On the Internet Explorer **Tools** menu, click **Internet Options**. 2. In the **Internet Options** dialog box, click the **Security** tab, and then click **Internet**.		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	3. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 4. Click **Local intranet**. 5. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High. 6. Click **OK** to accept the changes and return to Internet Explorer. **Note** If no slider is visible, click **Default Level**, and then move the slider to **High**. **Note** Setting the level to High may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly even with the security setting set to High. **Impact of workaround.** There are side effects to blocking ActiveX Controls and Active Scripting. Many websites on the Internet or an intranet use ActiveX or Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX Controls to provide menus, ordering forms, or even account statements. Blocking ActiveX Controls or Active Scripting is a global setting that affects all Internet and intranet sites. If		

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	you do not want to block ActiveX Controls or Active Scripting for such sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone". • **Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone** You can help protect against exploitation of these vulnerabilities by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone. To do this, perform the following steps: 1. In Internet Explorer, click **Internet Options** on the **Tools** menu. 2. Click the **Security** tab. 3. Click **Internet**, and then click **Custom Level**. 4. Under **Settings**, in the **Scripting** section, under **Active Scripting**, click **Prompt** or **Disable**, and then click **OK**. 5. Click **Local intranet**, and then click **Custom Level**.		

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

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

CVE ID	Vulnerability Description	Maximum Severity Rating	Vulnerability Impact
	4. In the **Add this website to the zone** box, type the URL of a site that you trust, and then click **Add**. 5. Repeat these steps for each site that you want to add to the zone. 6. Click **OK** two times to accept the changes and return to Internet Explorer. **Note** Add any sites that you trust not to take malicious action on your system. Two sites in particular that you may want to add are ***.windowsupdate.microsoft.com** and ***.update.microsoft.com**. These are the sites that will host the update, and they require an ActiveX control to install the update. **Revision:** 1.0 2017-07-11T07:00:00 Information Published.		

Affected Software

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

ADV170009						
Product	KB Article	Severity	Impact	Supersedence	CVSS Score Set	Restart Required
Adobe Flash Player on Windows 10 for 32-bit Systems	4025376 (Security Update)	Critical	Remote Code Execution	4022730	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 for x64-based Systems	4025376 (Security Update)	Critical	Remote Code Execution	4022730	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1511 for 32-bit Systems	4025376 (Security Update)	Critical	Remote Code Execution	4022730	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1511 for x64-based Systems	4025376 (Security Update)	Critical	Remote Code Execution	4022730	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1607 for 32-bit Systems	4025376 (Security Update)	Critical	Remote Code Execution	4022730	Base: N/A Temporal: N/A Vector: N/A	Yes

ADV170009						
Adobe Flash Player on Windows 10 Version 1607 for x64-based Systems	4025376 (Security Update)	Critical	Remote Code Execution	4022730	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for 32-bit Systems	4025376 (Security Update)	Critical	Remote Code Execution	4022730	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 10 Version 1703 for x64-based Systems	4025376 (Security Update)	Critical	Remote Code Execution	4022730	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for 32-bit systems	4025376 (Security Update)	Critical	Remote Code Execution	4022730	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows 8.1 for x64-based systems	4025376 (Security Update)	Critical	Remote Code Execution	4022730	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows RT 8.1	4025376 (Security Update)	Critical	Remote Code Execution	4022730	Base: N/A Temporal:	Yes

ADV170009						
					N/A Vector: N/A	
Adobe Flash Player on Windows Server 2012	4025376 (Security Update)	Critical	Remote Code Execution	4022730	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2012 R2	4025376 (Security Update)	Critical	Remote Code Execution	4022730	Base: N/A Temporal: N/A Vector: N/A	Yes
Adobe Flash Player on Windows Server 2016	4025376 (Security Update)	Critical	Remote Code Execution	4022730	Base: N/A Temporal: N/A Vector: N/A	Yes

声　明

==========

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

关于绿盟科技

==========

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

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

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

绿盟科技官方微博二维码

绿盟科技官方微信二维码