EN Ez a tartalom nem érhető el az Ön nyelvén, csak angol nyelven.

Microsoft Security Bulletin Summary for March 2017

Published: March 14, 2017 | Updated: August 8, 2017

Version: 4.0

This bulletin summary lists security bulletins released for March 2017.

For information about how to receive automatic notifications whenever Microsoft security bulletins are issued, visit Microsoft Technical Security Notifications.

Microsoft also provides information to help customers prioritize monthly security updates with any non-security updates that are being released on the same day as the monthly security updates. Please see the section, **Other Information**.

As a reminder, the Security Updates Guide will be replacing security bulletins. Please see our blog post, Furthering our commitment to security updates, for more details.

On this page

Executive Summaries

The following table summarizes the security bulletins for this month in order of severity.

For details on affected software, see the next section, **Affected Software**.

Bulletin ID	Bulletin Title and Executive Summary	Maximum Severity Rating and Vulnerability Impact	Restart Requirement	Known Issues	Affected Software
MS17-006	**Cumulative Security Update for Internet Explorer (4013073)** This security update resolves vulnerabilities in Internet Explorer. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited these vulnerabilities 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 control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Critical Remote Code Execution	Requires restart	----------	Microsoft Windows, Microsoft Internet Explorer
MS17-007	**Cumulative Security Update for Microsoft Edge (4013071)** This security update resolves vulnerabilities in Microsoft Edge. These vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Microsoft Edge. An attacker who successfully exploited these vulnerabilities could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Critical Remote Code Execution	Requires restart	----------	Microsoft Windows, Microsoft Edge
MS17-008	**Security Update for Windows Hyper-V (4013082)** This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an authenticated attacker on a guest operating system runs a specially crafted application that causes the Hyper-V host operating system to execute arbitrary code. Customers who have not enabled the Hyper-V role are not affected.	Critical Remote Code Execution	Requires restart	----------	Microsoft Windows
MS17-009	**Security Update for Microsoft Windows PDF Library (4010319)** This security update resolves a vulnerability in Microsoft	Critical Remote Code Execution	Requires restart	----------	Microsoft Windows

	Windows. The vulnerability could allow remote code execution if a user views specially crafted PDF content online or opens a specially crafted PDF document.				
MS17-010	**Security Update for Microsoft Windows SMB Server (4013389)** This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.	Critical Remote Code Execution	Requires restart	----------	Microsoft Windows
MS17-011	**Security Update for Microsoft Uniscribe (4013076)** This security update resolves vulnerabilities in Windows Uniscribe. The most severe of these vulnerabilities could allow remote code execution if a user visits a specially crafted website or opens a specially crafted document. 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.	Critical Remote Code Execution	Requires restart	----------	Microsoft Windows
MS17-012	**Security Update for Microsoft Windows (4013078)** This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker runs a specially crafted application that connects to an iSNS Server and then issues malicious requests to the server.	Critical Remote Code Execution	Requires restart	----------	Microsoft Windows
MS17-013	**Security Update for Microsoft Graphics Component (4013075)** This security update resolves vulnerabilities in Microsoft Windows, Microsoft Office, Skype for Business, Microsoft Lync, and Microsoft Silverlight. The most severe of these vulnerabilities could allow remote code execution if a user either visits a specially crafted website or opens a specially crafted document. 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.	Critical Remote Code Execution	Requires restart	----------	Microsoft Windows Microsoft Office, Skype for Business, Microsoft Lync, Microsoft Silverlight
MS17-014	**Security Update for Microsoft Office (4013241)** This security update resolves vulnerabilities in Microsoft Office. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file. An attacker who successfully exploited the vulnerabilities could run arbitrary code in the context of the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.	Important Remote Code Execution	May require restart	----------	Microsoft Office, Microsoft Office Services and Web Apps, Microsoft Server Software, Microsoft Communications Platforms and Software
MS17-015	**Security Update for Microsoft Exchange Server (4013242)** This security update resolves a vulnerability in Microsoft Exchange Outlook Web Access (OWA). The vulnerability could allow remote code execution in Exchange Server if an attacker sends an email with a specially crafted attachment to a vulnerable Exchange server.	Important Remote Code Execution	Requires restart	----------	Microsoft Exchange
MS17-016	**Security Update for Windows IIS (4013074)** This security update resolves a vulnerability in Microsoft Internet Information Services (IIS). The vulnerability could allow elevation of privilege if a user clicks a specially crafted URL which is hosted by an affected Microsoft IIS server. An attacker who successfully exploited this vulnerability could potentially execute scripts in the user's browser to obtain information from web sessions.	Important Remote Code Execution	Requires restart	----------	Microsoft Windows
MS17-017	**Security Update for Windows Kernel (4013081)** This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker runs a specially crafted application.	Important Elevation of Privilege	Requires restart	----------	Microsoft Windows

MS17-018	**Security Update for Windows Kernel-Mode Drivers (4013083)** This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application that could exploit the vulnerabilities and take control of an affected system.	Important Elevation of Privilege	Requires restart	----------	Microsoft Windows
MS17-019	**Security Update for Active Directory Federation Services (4010320)** This security update resolves a vulnerability in Active Directory Federation Services (ADFS). The vulnerability could allow information disclosure if an attacker sends a specially crafted request to an ADFS server, allowing the attacker to read sensitive information about the target system.	Important Information Disclosure	Requires restart	----------	Microsoft Windows
MS17-020	**Security Update for Windows DVD Maker (3208223)** This security update resolves an information disclosure vulnerability in Windows DVD Maker. The vulnerability could allow an attacker to obtain information to further compromise a target system.	Important Information Disclosure	Requires restart	----------	Microsoft Windows
MS17-021	**Security Update for Windows DirectShow (4010318)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow an information disclosure if Windows DirectShow opens specially crafted media content that is hosted on a malicious website. An attacker who successfully exploited the vulnerability could obtain information to further compromise a target system.	Important Information Disclosure	Requires restart	----------	Microsoft Windows
MS17-022	**Security Update for Microsoft XML Core Services (4010321)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure if a user visits a malicious website. However, in all cases an attacker would have no way to force a user to click a specially crafted link. An attacker would have to convince a user to click the link, typically by way of an enticement in an email or Instant Messenger message.	Important Information Disclosure	Requires restart	----------	Microsoft Windows
MS17-023	**Security Update for Adobe Flash Player (**4014329) This security update resolves vulnerabilities in Adobe Flash Player when installed on all supported editions of Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, Windows 10, and Windows Server 2016.	Critical Remote Code Execution	Requires restart	----------	Microsoft Windows, Adobe Flash Player

Exploitability Index

The following table provides an exploitability assessment of each of the vulnerabilities addressed this month. The vulnerabilities are listed in order of bulletin ID then CVE ID. Only vulnerabilities that have a severity rating of Critical or Important in the bulletins are included.

How do I use this table?

Use this table to learn about the likelihood of code execution and denial of service exploits within 30 days of security bulletin release, for each of the security updates that you may need to install. Review each of the assessments below, in accordance with your specific configuration, to prioritize your deployment of this month's updates. For more information about what these ratings mean, and how they are determined, please see Microsoft Exploitability Index.

In the columns below, "Latest Software Release" refers to the subject software, and "Older Software Releases" refers to all older, supported releases of the subject software, as listed in the "Affected Software" and "Non-Affected Software" tables in the bulletin.

CVE ID	Vulnerability Title	Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment

MS17-006: Cumulative Security Update for Internet Explorer (4013073)				
CVE-2017-0008	Internet Explorer Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0009	Microsoft Browser Information Disclosure Vulnerability	1 - Exploitation More Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0012	Microsoft Browser Spoofing Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2017-0018	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0033	Microsoft Browser Spoofing Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0037	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0040	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0049	Scripting Engine Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0059	Internet Explorer Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0130	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0149	Internet Explorer Memory Corruption Vulnerability	0 - Exploitation Detected	0 - Exploitation Detected	Not applicable
CVE-2017-0154	Internet Explorer Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS17-007: Cumulative Security Update for Microsoft Edge (4013071)				
CVE-2017-0009	Microsoft Browser Information Disclosure Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0010	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0011	Microsoft Edge Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2017-0012	Microsoft Browser Spoofing Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2017-0015	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0017	Microsoft Edge Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2017-0023	Microsoft PDF Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0032	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0033	Microsoft Browser Spoofing Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0034	Microsoft Edge Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable

CVE-2017-0035	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0037	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0065	Microsoft Browser Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2017-0066	Microsoft Edge Security Feature Bypass Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2017-0067	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0068	Microsoft Edge Information Disclosure Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2017-0069	Microsoft Edge Spoofing Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2017-0070	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0071	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0094	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0131	Scripting Engine Memory Corruption Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2017-0132	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0133	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0134	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0135	Microsoft Edge Security Feature Bypass	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2017-0136	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0137	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0138	Scripting Engine Memory Corruption Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2017-0140	Microsoft Edge Security Feature Bypass	2 - Exploitation Less Likely	4 - Not affected	Not applicable
CVE-2017-0141	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0150	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0151	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
MS17-008: Security Update for Windows Hyper-V (4013082)				
CVE-2017-0021	Hyper-V vSMB Remote Code	2 - Exploitation Less Likely	4 - Not affected	Not applicable

	Execution Vulnerability			
CVE-2017-0051	Microsoft Hyper-V Network Switch Denial of Service Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2017-0074	Hyper-V Denial of Service Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Permanent
CVE-2017-0075	Hyper-V Remote Code Execution Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0076	Hyper-V Denial of Service Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2017-0095	Hyper-V vSMB Remote Code Execution Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0096	Hyper-V Information Disclosure Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2017-0097	Hyper-V Denial of Service Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Permanent
CVE-2017-0098	Hyper-V Denial of Service Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2017-0099	Hyper-V Denial of Service Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Permanent
CVE-2017-0109	Hyper-V Remote Code Execution Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS17-009: Security Update for Microsoft Windows PDF Library (4010319)				
CVE-2017-0023	Microsoft PDF Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS17-010: Security Update for Microsoft Windows SMB Server (4013389)				
CVE-2017-0143	Windows SMB Remote Code Execution Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0144	Windows SMB Remote Code Execution Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0145	Windows SMB Remote Code Execution Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0146	Windows SMB Remote Code Execution Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0147	Windows SMB Information Disclosure Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0148	Windows SMB Remote Code Execution Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS17-011: Security Update for Microsoft Uniscribe (4013076)				
CVE-2017-0072	Uniscribe Remote Code Execution Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2017-0083	Uniscribe Remote Code Execution Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0084	Uniscribe Remote Code Execution Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable

CVE-2017-0085	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0086	Uniscribe Remote Code Execution Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2017-0087	Uniscribe Remote Code Execution Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2017-0088	Uniscribe Remote Code Execution Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2017-0089	Uniscribe Remote Code Execution Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2017-0090	Uniscribe Remote Code Execution Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2017-0091	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0092	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0111	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0112	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0113	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0114	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0115	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0116	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0117	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0118	Uniscribe Information Disclosure Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2017-0119	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0120	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0121	Uniscribe Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0122	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0123	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0124	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0125	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable

CVE-2017-0126	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0127	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0128	Uniscribe Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
MS17-012: Security Update for Microsoft Windows (4013078)				
CVE-2017-0007	Device Guard Security Feature Bypass Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0016	SMBv2/SMBv3 Null Dereference Denial of Service Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0039	Windows DLL Loading Remote Code Execution Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2017-0057	Windows DNS Query Information Disclosure Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2017-0100	Windows HelpPane Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0104	iSNS Server Memory Corruption Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS17-013: Security Update for Microsoft Graphics Component (4013075)				
CVE-2017-0001	Windows GDI Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0005	Windows GDI Elevation of Privilege Vulnerability	1 - Exploitation More Likely	0 – Exploitation Detected	Not applicable
CVE-2017-0014	GDI+ Remote Code Execution Vulnerability	2 - Exploitation Less Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0025	Windows GDI Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0038	Windows Graphics Component Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0047	Windows GDI Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0060	GDI+ Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0061	Microsoft Color Management Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
CVE-2017-0062	GDI+ Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0063	Microsoft Color Management Information Disclosure Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2017-0073	Windows GDI+ Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0108	Windows Graphics Component	4 - Not affected	2 - Exploitation Less Likely	Not applicable

	Remote Code Execution Vulnerability			
MS17-014: Security Update for Microsoft Office (4013241)				
CVE-2017-0006	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2017-0019	Microsoft Office Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0020	Microsoft Office Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0027	Microsoft Office Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0029	Microsoft Office Denial of Service Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2017-0030	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2017-0031	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2017-0052	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2017-0053	Microsoft Office Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0105	Microsoft Office Information Disclosure Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2017-0107	Microsoft SharePoint XSS Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2017-0129	Microsoft Lync for Mac Certificate Validation Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
MS17-015: Security Update for Microsoft Exchange Server (4013242)				
CVE-2017-0110	Microsoft Exchange Server Elevation of Privilege Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS17-016: Security Update for Windows IIS (4013074)				
CVE-2017-0055	Microsoft IIS Server XSS Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS17-017: Security Update for Windows Kernel (4013081)				
CVE-2017-0050	Windows Kernel Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0101	Windows Elevation of Privilege Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Permanent
CVE-2017-0102	Windows Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0103	Windows Registry Elevation of Privilege Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
MS17-018: Security Update for Windows Kernel-Mode Drivers (4013083)				

CVE-2017-0024	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2017-0026	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0056	Win32k Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0078	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2017-0079	Win32k Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0080	Win32k Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Permanent
CVE-2017-0081	Win32k Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2017-0082	Win32k Elevation of Privilege Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
MS17-019: Security Update for Active Directory Federation Services (4010320)				
CVE-2017-0043	Microsoft Active Directory Federation Services Information Disclosure Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Temporary
MS17-020: Security Update for Windows DVD Maker (3208223)				
CVE-2017-0045	Windows DVD Maker Cross-Site Request Forgery Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Not applicable
MS17-021: Security Update for Windows DirectShow (4010318)				
CVE-2017-0042	Windows DirectShow Information Disclosure Vulnerabitliy	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS17-022: Security Update for Microsoft XML Core Services (4010321)				
CVE-2017-0022	Microsoft XML Core Services Information Disclosure Vulnerability	0 - Exploitation Detected	0 - Exploitation Detected	Not applicable
MS17-023: Security Update for Adobe Flash Player (4014329)				
APSB17-07	See Adobe Security Bulletin APSB17-07 for vulnerability severity and update priority ratings	---------	---------	Not applicable

Affected Software

The following tables list the bulletins in order of major software category and severity.

Use these tables to learn about the security updates that you may need to install. You should review each software program or component listed to see whether any security updates pertain to your installation. If a software program or component is listed, then the severity rating of the software update is also listed.

Note You may have to install several security updates for a single vulnerability. Review the whole column for each bulletin identifier that is listed to verify the updates that you have to install, based on the programs or components that you have installed on your system.

Windows Operating Systems and Components (Table 1 of 2)

Windows Vista								
Bulletin Identifier	**MS17-006**	**MS17-007**	**MS17-008**	**MS17-009**	**MS17-010**	**MS17-011**	**MS17-012**	**MS17-013**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**None**	**Critical**	**Critical**	**Important**	**Critical**
Windows Vista Service Pack 2	Internet Explorer 9 (4012204) (Critical) Microsoft Internet Messaging API (3218362) (Important)	Not applicable	Not applicable	Not applicable	Windows Vista Service Pack 2 (4012598) (Critical)	Windows Vista Service Pack 2 (4012583) (Critical)	Windows Vista Service Pack 2 (3217587) (Important)	Windows Vista Service Pack 2 (4017018) (Critical) Windows Vista Service Pack 2 (4012584) (Important) Windows Vista Service Pack 2 (4012497) (Important)
Windows Vista x64 Edition Service Pack 2	Internet Explorer 9 (4012204) (Critical) Microsoft Internet Messaging API (3218362) (Important)	Not applicable	Windows Vista x64 Edition Service Pack 2 (3211306) (Critical)	Not applicable	Windows Vista x64 Edition Service Pack 2 (4012598) (Critical)	Windows Vista x64 Edition Service Pack 2 (4012583) (Critical)	Windows Vista x64 Edition Service Pack 2 (3217587) (Important)	Windows Vista x64 Edition Service Pack 2 (4017018) (Critical) Windows Vista x64 Edition Service Pack 2 (4012584) (Important) Windows Vista x64 Edition Service Pack 2 (4012497) (Important)
Windows Server 2008								
Bulletin Identifier	**MS17-006**	**MS17-007**	**MS17-008**	**MS17-009**	**MS17-010**	**MS17-011**	**MS17-012**	**MS17-013**
Aggregate Severity Rating	**Important**	**None**	**Critical**	**None**	**Critical**	**Critical**	**Critical**	**Critical**
Windows Server 2008 for 32-bit Systems Service Pack 2	Internet Explorer 9 (4012204) (Moderate) Microsoft Internet Messaging API (3218362) (Important)	Not applicable	Not applicable	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (4012598) (Critical)	Windows Server 2008 for 32-bit Systems Service Pack 2 (4012583) (Critical)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3217587) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2	Windows Server 2008 for 32-bit Systems Service Pack 2 (4017018) (Critical) Windows Server 2008 for 32-bit Systems Service Pack 2 (4012584)

							(4012021) (Critical)	(Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (4012497) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Internet Explorer 9 (4012204) (Moderate) Microsoft Internet Messaging API (3218362) (Important)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3211306) (Critical)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (4012598) (Critical)	Windows Server 2008 for x64-based Systems Service Pack 2 (4012583) (Critical)	Windows Server 2008 for x64-based Systems Service Pack 2 (3217587) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (4012021) (Critical)	Windows Server 2008 for x64-based Systems Service Pack 2 (4017018) (Critical) Windows Server 2008 for x64-based Systems Service Pack 2 (4012584) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (4012497) (Important)
Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Not applicable	Not applicable	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (4012598) (Critical)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (4012583) (Critical)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3217587) (Important)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (4017018) (Critical) Windows Server 2008 for Itanium-based Systems Service Pack 2 (4012584) (Important) Windows Server 2008 for Itanium-based Systems Service Pack 2 (4012497) (Important)
Windows 7								
Bulletin Identifier	**MS17-006**	**MS17-007**	**MS17-008**	**MS17-009**	**MS17-010**	**MS17-011**	**MS17-012**	**MS17-013**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**None**	**Critical**	**Critical**	**Important**	**Critical**
Windows 7 for 32-bit	Internet Explorer 11	Not applicable	Not applicable	Not applicable	Windows 7 for 32-bit	Windows 7 for 32-bit	Windows 7 for 32-bit	Windows 7 for 32-bit

Systems Service Pack 1 Security Only	(4012204) (Critical)				Systems Service Pack 1 (4012212) (Critical)	Systems Service Pack 1 (4012212) (Critical)	Systems Service Pack 1 (4012212) (Important)	Systems Service Pack 1 (4012212) (Critical)
Windows 7 for 32-bit Systems Service Pack 1 Monthly Rollup	Internet Explorer 11 (4012215) (Critical)	Not applicable	Not applicable	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (4012215) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (4012215) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (4012215) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (4012215) (Critical)
Windows 7 for x64-based Systems Service Pack 1 Security Only	Internet Explorer 11 (4012204) (Critical)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (4012212) (Critical)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (4012212) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (4012212) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (4012212) (Important)	Windows 7 for x64-based Systems Service Pack 1 (4012212) (Critical)
Windows 7 for x64-based Systems Service Pack 1 Monthly Rollup	Internet Explorer 11 (4012215) (Critical)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (4012215) (Critical)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (4012215) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (4012215) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (4012215) (Important)	Windows 7 for x64-based Systems Service Pack 1 (4012215) (Critical)
Windows Server 2008 R2								
Bulletin Identifier	**MS17-006**	**MS17-007**	**MS17-008**	**MS17-009**	**MS17-010**	**MS17-011**	**MS17-012**	**MS17-013**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**None**	**Critical**	**Critical**	**Critical**	**Critical**
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Security Only	Internet Explorer 11 (4012204) (Moderate)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012212) (Critical)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012212) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012212) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012212) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012212) (Critical)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Monthly Rollup	Internet Explorer 11 (4012215) (Moderate)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012215) (Critical)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012215) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012215) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012215) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012215) (Critical)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Security Only	Not applicable	Not applicable	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012212) (Critical)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012212) (Critical)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012212) (Critical)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012212) (Critical)

Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Monthly Rollup	Not applicable	Not applicable	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012215) (Critical)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012215) (Critical)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012215) (Critical)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012215) (Critical)
Windows 8.1								
Bulletin Identifier	**MS17-006**	**MS17-007**	**MS17-008**	**MS17-009**	**MS17-010**	**MS17-011**	**MS17-012**	**MS17-013**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**Critical**	**Important**	**Important**	**Critical**
Windows 8.1 for 32-bit Systems Security Only	Internet Explorer 11 (4012204) (Critical)	Not applicable	Not applicable	Windows 8.1 for 32-bit Systems (4012213) (Critical)	Windows 8.1 for 32-bit Systems (4012213) (Critical)	Windows 8.1 for 32-bit Systems (4012213) (Important)	Windows 8.1 for 32-bit Systems (4012213) (Important)	Windows 8.1 for 32-bit Systems (4012213) (Critical)
Windows 8.1 for 32-bit Systems Monthly Rollup	Internet Explorer 11 (4012216) (Critical)	Not applicable	Not applicable	Windows 8.1 for 32-bit Systems (4012216) (Critical)	Windows 8.1 for 32-bit Systems (4012216) (Critical)	Windows 8.1 for 32-bit Systems (4012216) (Important)	Windows 8.1 for 32-bit Systems (4012216) (Important)	Windows 8.1 for 32-bit Systems (4012216) (Critical)
Windows 8.1 for x64-based Systems Security Only	Internet Explorer 11 (4012204) (Critical)	Not applicable	Windows 8.1 for x64-based Systems (4012213) (Critical)	Windows 8.1 for x64-based Systems (4012213) (Critical)	Windows 8.1 for x64-based Systems (4012213) (Critical)	Windows 8.1 for x64-based Systems (4012213) (Important)	Windows 8.1 for x64-based Systems (4012213) (Important)	Windows 8.1 for x64-based Systems (4012213) (Critical)
Windows 8.1 for x64-based Systems Monthly Rollup	Internet Explorer 11 (4012216) (Critical)	Not applicable	Windows 8.1 for x64-based Systems (4012216) (Critical)	Windows 8.1 for x64-based Systems (4012216) (Critical)	Windows 8.1 for x64-based Systems (4012216) (Critical)	Windows 8.1 for x64-based Systems (4012216) (Important)	Windows 8.1 for x64-based Systems (4012216) (Important)	Windows 8.1 for x64-based Systems (4012216) (Critical)
Windows Server 2012 and Windows Server 2012 R2								
Bulletin Identifier	**MS17-006**	**MS17-007**	**MS17-008**	**MS17-009**	**MS17-010**	**MS17-011**	**MS17-012**	**MS17-013**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**Critical**	**Critical**	**Important**	**Critical**	**Critical**
Windows Server 2012 Security Only	Internet Explorer 10 (4012204) (Moderate)	Not applicable	Windows Server 2012 (4012214) (Critical)	Windows Server 2012 (4012214) (Critical)	Windows Server 2012 (4012214) (Critical)	Windows Server 2012 (4012214) (Important)	Windows Server 2012 (4012214) (Critical)	Windows Server 2012 (4012214) (Critical)
Windows Server 2012 Monthly Rollup	Internet Explorer 10 (4012217) (Moderate)	Not applicable	Windows Server 2012 (4012217) (Critical)	Windows Server 2012 (4012217) (Critical)	Windows Server 2012 (4012217) (Critical)	Windows Server 2012 (4012217) (Important)	Windows Server 2012 (4012217) (Critical)	Windows Server 2012 (4012217) (Critical)
Windows Server 2012 R2	Internet Explorer 11 (4012204) (Moderate)	Not applicable	Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2

Security Only			(4012213) (Critical)	(4012213) (Critical)	(4012213) (Critical)	(4012213) (Important)	(4012213) (Critical)	(4012213) (Critical)
Windows Server 2012 R2 Monthly Rollup	Internet Explorer 11 (4012216) (Moderate)	Not applicable	Windows Server 2012 R2 (4012216) (Critical)	Windows Server 2012 R2 (4012216) (Critical)	Windows Server 2012 R2 (4012216) (Critical)	Windows Server 2012 R2 (4012216) (Important)	Windows Server 2012 R2 (4012216) (Critical)	Windows Server 2012 R2 (4012216) (Critical)
Windows RT 8.1								
Bulletin Identifier	**MS17-006**	**MS17-007**	**MS17-008**	**MS17-009**	**MS17-010**	**MS17-011**	**MS17-012**	**MS17-013**
Aggregate Severity Rating	**Critical**	**None**	**None**	**Critical**	**Critical**	**Important**	**Important**	**Critical**
Windows RT 8.1 Monthly Rollup	Internet Explorer 11 (4012216) (Critical)	Not applicable	Not applicable	Windows RT 8.1 (4012216) (Critical)	Windows RT 8.1 (4012216) (Critical)	Windows RT 8.1 (4012216) (Important)	Windows RT 8.1 (4012216) (Important)	Windows RT 8.1 (4012216) (Critical)
Windows 10								
Bulletin Identifier	**MS17-006**	**MS17-007**	**MS17-008**	**MS17-009**	**MS17-010**	**MS17-011**	**MS17-012**	**MS17-013**
Aggregate Severity Rating	**Critical**	**Critical**	**Critical**	**Critical**	**Critical**	**Important**	**Important**	**Critical**
Windows 10 for 32-bit Systems	Internet Explorer 11 (4012606) (Critical)	Microsoft Edge (4025338) (Critical)	Not applicable	Windows 10 for 32-bit Systems (4012606) (Critical)	Windows 10 for 32-bit Systems (4012606) (Critical)	Windows 10 for 32-bit Systems (4012606) (Important)	Windows 10 for 32-bit Systems (4012606) (Important)	Windows 10 for 32-bit Systems (4012606) (Critical)
Windows 10 for x64-based Systems	Internet Explorer 11 (4012606) (Critical)	Microsoft Edge (4025338) (Critical)	Windows 10 for x64-based Systems (4012606) (Critical)	Windows 10 for x64-based Systems (4012606) (Critical)	Windows 10 for x64-based Systems (4012606) (Critical)	Windows 10 for x64-based Systems (4012606) (Important)	Windows 10 for x64-based Systems (4012606) (Important)	Windows 10 for x64-based Systems (4012606) (Critical)
Windows 10 Version 1511 for 32-bit Systems	Internet Explorer 11 (4013198) (Critical)	Microsoft Edge (4025344) (Critical)	Not applicable	Windows 10 Version 1511 for 32-bit Systems (4013198) (Critical)	Windows 10 Version 1511 for 32-bit Systems (4013198) (Critical)	Windows 10 Version 1511 for 32-bit Systems (4013198) (Important)	Windows 10 Version 1511 for 32-bit Systems (4013198) (Important)	Windows 10 Version 1511 for 32-bit Systems (4013198) (Critical)
Windows 10 Version 1511 for x64-based Systems	Internet Explorer 11 (4013198) (Critical)	Microsoft Edge (4025344) (Critical)	Windows 10 Version 1511 for x64-based Systems (4013198) (Critical)	Windows 10 Version 1511 for x64-based Systems (4013198) (Critical)	Windows 10 Version 1511 for x64-based Systems (4013198) (Critical)	Windows 10 Version 1511 for x64-based Systems (4013198) (Important)	Windows 10 Version 1511 for x64-based Systems (4013198) (Important)	Windows 10 Version 1511 for x64-based Systems (4013198) (Critical)
Windows 10 Version 1607 for 32-bit Systems	Internet Explorer 11 (4013429) (Critical)	Microsoft Edge (4025339) (Critical)	Not applicable	Windows 10 Version 1607 for 32-bit Systems (4013429) (Critical)	Windows 10 Version 1607 for 32-bit Systems (4013429) (Critical)	Windows 10 Version 1607 for 32-bit Systems (4013429) (Important)	Windows 10 Version 1607 for 32-bit Systems (4013429) (Important)	Windows 10 Version 1607 for 32-bit Systems (4013429) (Critical)
Windows 10 Version 1607 for x64-based Systems	Internet Explorer 11 (4013429) (Critical)	Microsoft Edge (4025339) (Critical)	Windows 10 Version 1607 for x64-based Systems (4013429) (Critical)	Windows 10 Version 1607 for x64-based Systems (4013429) (Critical)	Windows 10 Version 1607 for x64-based Systems (4013429) (Critical)	Windows 10 Version 1607 for x64-based Systems (4013429) (Important)	Windows 10 Version 1607 for x64-based Systems (4013429) (Important)	Windows 10 Version 1607 for x64-based Systems (4013429) (Critical)

Windows 10 Version 1703 for 32-bit Systems	Not applicable	Microsoft Edge (4025342) (Critical)	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Windows 10 Version 1703 for x64-based Systems	Not applicable	Microsoft Edge (4025342) (Critical)	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2016								
Bulletin Identifier	**MS17-006**	**MS17-007**	**MS17-008**	**MS17-009**	**MS17-010**	**MS17-011**	**MS17-012**	**MS17-013**
Aggregate Severity Rating	**Moderate**	**Moderate**	**Critical**	**Critical**	**Critical**	**Important**	**Critical**	**Critical**
Windows Server 2016 for x64-based Systems	Internet Explorer 11 (4013429) (Moderate)	Microsoft Edge (4013429) (Moderate)	Windows Server 2016 for x64-based Systems (4013429) (Critical)	Windows Server 2016 for x64-based Systems (4013429) (Critical)	Windows Server 2016 for x64-based Systems (4013429) (Critical)	Windows Server 2016 for x64-based Systems (4013429) (Important)	Windows Server 2016 for x64-based Systems (4013429) (Critical)	Windows Server 2016 for x64-based Systems (4013429) (Critical)
Server Core installation option								
Bulletin Identifier	**MS17-006**	**MS17-007**	**MS17-008**	**MS17-009**	**MS17-010**	**MS17-011**	**MS17-012**	**MS17-013**
Aggregate Severity Rating	**None**	**None**	**Critical**	**None**	**Critical**	**Critical**	**Critical**	**Critical**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	Not applicable	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (4012598) (Critical)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (4012583) (Critical)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3217587) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (4017018) (Critical) Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (4012584) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (4012497) (Important)
Windows Server 2008 for	Not applicable	Not applicable	Windows Server 2008 for x64-based	Not applicable	Windows Server 2008 for x64-based	Windows Server 2008 for x64-based	Windows Server 2008 for x64-based	Windows Server 2008 for x64-based

x64-based Systems Service Pack 2 (Server Core installation)			Systems Service Pack 2 (Server Core installation) (3211306) (Critical)		Systems Service Pack 2 (Server Core installation) (4012598) (Critical)	Systems Service Pack 2 (Server Core installation) (4012583) (Critical)	Systems Service Pack 2 (Server Core installation) (3217587) (Important)	Systems Service Pack 2 (Server Core installation) (4017018) (Critical) Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (4012584) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (4012497) (Important)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Security Only	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012212) (Critical)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012212) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012212) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012212) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012212) (Critical)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Monthly Rollup	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012215) (Critical)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012215) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012215) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012215) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012215) (Critical)
Windows Server 2012 (Server Core installation) Security Only	Not applicable	Not applicable	Windows Server 2012 (Server Core installation) (4012214) (Critical)	Not applicable	Windows Server 2012 (Server Core installation) (4012214) (Critical)	Windows Server 2012 (Server Core installation) (4012214) (Important)	Windows Server 2012 (Server Core installation) (4012214) (Critical)	Windows Server 2012 (Server Core installation) (4012214) (Critical)
Windows Server 2012 (Server Core installation) Monthly Rollup	Not applicable	Not applicable	Windows Server 2012 (Server Core installation) (4012217) (Critical)	Not applicable	Windows Server 2012 (Server Core installation) (4012217) (Critical)	Windows Server 2012 (Server Core installation) (4012217) (Important)	Windows Server 2012 (Server Core installation) (4012217) (Critical)	Windows Server 2012 (Server Core installation) (4012217) (Critical)
Windows	Not applicable	Not applicable	Windows	Not applicable	Windows	Windows	Windows	Windows

Server 2012 R2 (Server Core installation) Security Only			Server 2012 R2 (Server Core installation) (4012213) (Critical)		Server 2012 R2 (Server Core installation) (4012213) (Critical)	Server 2012 R2 (Server Core installation) (4012213) (Important)	Server 2012 R2 (Server Core installation) (4012213) (Critical)	Server 2012 R2 (Server Core installation) (4012213) (Critical)
Windows Server 2012 R2 (Server Core installation) Monthly Rollup	Not applicable	Not applicable	Windows Server 2012 R2 (Server Core installation) (4012216) (Critical)	Not applicable	Windows Server 2012 R2 (Server Core installation) (4012216) (Critical)	Windows Server 2012 R2 (Server Core installation) (4012216) (Important)	Windows Server 2012 R2 (Server Core installation) (4012216) (Critical)	Windows Server 2012 R2 (Server Core installation) (4012216) (Critical)
Windows Server 2016 for x64-based Systems (Server Core installation)	Not applicable	Not applicable	Windows Server 2016 for x64-based Systems (Server Core installation) (4013429) (Critical)	Not applicable	Windows Server 2016 for x64-based Systems (Server Core installation) (4013429) (Critical)	Windows Server 2016 for x64-based Systems (Server Core installation) (4013429) (Important)	Windows Server 2016 for x64-based Systems (Server Core installation) (4013429) (Critical)	Windows Server 2016 for x64-based Systems (Server Core installation) (4013429) (Critical)

Note for MS17-013

This bulletin spans more than one software category. See other tables in this section for additional affected software.

Windows Operating Systems and Components (Table 2 of 2)

Windows Vista								
Bulletin Identifier	**MS17-016**	**MS17-017**	**MS17-018**	**MS17-019**	**MS17-020**	**MS17-021**	**MS17-022**	**MS17-023**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**Important**	**Important**	**Important**	**None**
Windows Vista Service Pack 2	Windows Vista Service Pack 2 (4012373) (Important)	Windows Vista Service Pack 2 (4011981) (Important)	Windows Vista Service Pack 2 (4012497) (Important)	Not applicable	Windows Vista Service Pack 2 (3205715) (Important)	Windows Vista Service Pack 2 (3214051) (Important)	Microsoft XML Core Services 3.0 (3216916) (Important)	Not applicable
Windows Vista x64 Edition Service Pack 2	Windows Vista x64 Edition Service Pack 2 (4012373) (Important)	Windows Vista x64 Edition Service Pack 2 (4011981) (Important)	Windows Vista x64 Edition Service Pack 2 (4012497) (Important)	Not applicable	Windows Vista x64 Edition Service Pack 2 (3205715) (Important)	Windows Vista x64 Edition Service Pack 2 (3214051) (Important)	Microsoft XML Core Services 3.0 (3216916) (Important)	Not applicable
Windows Server 2008								
Bulletin Identifier	**MS17-016**	**MS17-017**	**MS17-018**	**MS17-019**	**MS17-020**	**MS17-021**	**MS17-022**	**MS17-023**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Important**	**None**	**Important**	**Important**	**None**
Windows Server 2008 for 32-bit Systems	Windows Server 2008 for 32-bit Systems Service Pack 2	Windows Server 2008 for 32-bit Systems Service Pack 2	Windows Server 2008 for 32-bit Systems Service Pack 2	Windows Server 2008 for 32-bit Systems Service Pack 2	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2	Microsoft XML Core Services 3.0 (3216916) (Important)	Not applicable

Service Pack 2	(4012373) (Important)	(4011981) (Important)	(4012497) (Important)	(3217882) (Important)		(3214051) (Important)		
Windows Server 2008 for x64-based Systems Service Pack 2	Windows Server 2008 for x64-based Systems Service Pack 2 (4012373) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (4011981) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (4012497) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (3217882) (Important)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3214051) (Important)	Microsoft XML Core Services 3.0 (3216916) (Important)	Not applicable
Windows Server 2008 for Itanium-based Systems Service Pack 2	Windows Server 2008 for Itanium-based Systems Service Pack 2 (4012373) (Important)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (4011981) (Important)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (4012497) (Important)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3217882) (Important)	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3214051) (Important)	Microsoft XML Core Services 3.0 (3216916) (Important)	Not applicable
Windows 7								
Bulletin Identifier	**MS17-016**	**MS17-017**	**MS17-018**	**MS17-019**	**MS17-020**	**MS17-021**	**MS17-022**	**MS17-023**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**Important**	**Important**	**Important**	**None**
Windows 7 for 32-bit Systems Service Pack 1 Security Only	Windows 7 for 32-bit Systems Service Pack 1 (4012212) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (4012212) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (4012212) (Important)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (4012212) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (4012212) (Important)	Microsoft XML Core Services 3.0 (4012212) (Important)	Not applicable
Windows 7 for 32-bit Systems Service Pack 1 Monthly Rollup	Windows 7 for 32-bit Systems Service Pack 1 (4012215) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (4012215) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (4012215) (Important)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (4012215) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (4012215) (Important)	Microsoft XML Core Services 3.0 (4012215) (Important)	Not applicable
Windows 7 for x64-based Systems Service Pack 1 Security Only	Windows 7 for x64-based Systems Service Pack 1 (4012212) (Important)	Windows 7 for x64-based Systems Service Pack 1 (4012212) (Important)	Windows 7 for x64-based Systems Service Pack 1 (4012212) (Important)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (4012212) (Important)	Windows 7 for x64-based Systems Service Pack 1 (4012212) (Important)	Microsoft XML Core Services 3.0 (4012212) (Important)	Not applicable
Windows 7 for x64-based Systems Service Pack 1 Monthly Rollup	Windows 7 for x64-based Systems Service Pack 1 (4012215) (Important)	Windows 7 for x64-based Systems Service Pack 1 (4012215) (Important)	Windows 7 for x64-based Systems Service Pack 1 (4012215) (Important)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (4012215) (Important)	Windows 7 for x64-based Systems Service Pack 1 (4012215) (Important)	Microsoft XML Core Services 3.0 (4012215) (Important)	Not applicable
Windows Server 2008 R2								
Bulletin Identifier	**MS17-016**	**MS17-017**	**MS17-018**	**MS17-019**	**MS17-020**	**MS17-021**	**MS17-022**	**MS17-023**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Important**	**None**	**Important**	**Important**	**None**

Windows Server 2008 R2 for x64-based Systems Service Pack 1 Security Only	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012212) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012212) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012212) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012212) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012212) (Important)	Microsoft XML Core Services 3.0 (4012212) (Important)	Not applicable
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Monthly Rollup	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012215) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012215) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012215) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012215) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (4012215) (Important)	Microsoft XML Core Services 3.0 (4012215) (Important)	Not applicable
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Security Only	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012212) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012212) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012212) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012212) (Important)	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012212) (Important)	Microsoft XML Core Services 3.0 (4012212) (Important)	Not applicable
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 Monthly Rollup	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012215) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012215) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012215) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012215) (Important)	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (4012215) (Important)	Microsoft XML Core Services 3.0 (4012215) (Important)	Not applicable
Windows 8.1								
Bulletin Identifier	**MS17-016**	**MS17-017**	**MS17-018**	**MS17-019**	**MS17-020**	**MS17-021**	**MS17-022**	**MS17-023**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**None**	**Important**	**Important**	**Critical**
Windows 8.1 for 32-bit Systems Security Only	Windows 8.1 for 32-bit Systems (4012213) (Important)	Windows 8.1 for 32-bit Systems (4012213) (Important)	Windows 8.1 for 32-bit Systems (4012213) (Important)	Not applicable	Not applicable	Windows 8.1 for 32-bit Systems (4012213) (Important)	Microsoft XML Core Services 3.0 (4012213) (Important)	Adobe Flash Player (4014329) (Critical)
Windows 8.1 for 32-bit Systems Monthly Rollup	Windows 8.1 for 32-bit Systems (4012216) (Important)	Windows 8.1 for 32-bit Systems (4012216) (Important)	Windows 8.1 for 32-bit Systems (4012216) (Important)	Not applicable	Not applicable	Windows 8.1 for 32-bit Systems (4012216) (Important)	Microsoft XML Core Services 3.0 (4012216) (Important)	Not applicable
Windows 8.1 for x64-based Systems Security Only	Windows 8.1 for x64-based Systems (4012213) (Important)	Windows 8.1 for x64-based Systems (4012213) (Important)	Windows 8.1 for x64-based Systems (4012213) (Important)	Not applicable	Not applicable	Windows 8.1 for x64-based Systems (4012213) (Important)	Microsoft XML Core Services 3.0 (4012213) (Important)	Adobe Flash Player (4014329) (Critical)
Windows	Windows 8.1	Windows 8.1	Windows 8.1	Not applicable	Not applicable	Windows 8.1	Microsoft XML	Not applicable

8.1 for x64-based Systems Monthly Rollup	for x64-based Systems (4012216) (Important)	for x64-based Systems (4012216) (Important)	for x64-based Systems (4012216) (Important)			for x64-based Systems (4012216) (Important)	Core Services 3.0 (4012216) (Important)	
Windows Server 2012 and Windows Server 2012 R2								
Bulletin Identifier	**MS17-016**	**MS17-017**	**MS17-018**	**MS17-019**	**MS17-020**	**MS17-021**	**MS17-022**	**MS17-023**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Important**	**None**	**Important**	**Important**	**Critical**
Windows Server 2012 Security Only	Windows Server 2012 (4012214) (Important)	Windows Server 2012 (4012214) (Important)	Windows Server 2012 (4012214) (Important)	Windows Server 2012 (4012214) (Important)	Not applicable	Windows Server 2012 (4015548) (Important)	Microsoft XML Core Services 3.0 (4012214) (Important)	Adobe Flash Player (4014329) (Critical)
Windows Server 2012 Monthly Rollup	Windows Server 2012 (4012217) (Important)	Windows Server 2012 (4012217) (Important)	Windows Server 2012 (4012217) (Important)	Windows Server 2012 (4012217) (Important)	Not applicable	Windows Server 2012 (4015551) (Important)	Microsoft XML Core Services 3.0 (4012217) (Important)	Not applicable
Windows Server 2012 R2 Security Only	Windows Server 2012 R2 (4012213) (Important)	Windows Server 2012 R2 (4012213) (Important)	Windows Server 2012 R2 (4012213) (Important)	Windows Server 2012 R2 (4012213) (Important)	Not applicable	Windows Server 2012 R2 (4012213) (Important)	Microsoft XML Core Services 3.0 (4012213) (Important)	Adobe Flash Player (4014329) (Critical)
Windows Server 2012 R2 Monthly Rollup	Windows Server 2012 R2 (4012216) (Important)	Windows Server 2012 R2 (4012216) (Important)	Windows Server 2012 R2 (4012216) (Important)	Windows Server 2012 R2 (4012216) (Important)	Not applicable	Windows Server 2012 R2 (4012216) (Important)	Microsoft XML Core Services 3.0 (4012216) (Important)	Not applicable
Windows RT 8.1								
Bulletin Identifier	**MS17-016**	**MS17-017**	**MS17-018**	**MS17-019**	**MS17-020**	**MS17-021**	**MS17-022**	**MS17-023**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**None**	**Important**	**Important**	**Critical**
Windows RT 8.1 Monthly Rollup	Windows RT 8.1 (4012216) (Important)	Windows RT 8.1 (4012216) (Important)	Windows RT 8.1 (4012216) (Important)	Not applicable	Not applicable	Windows RT 8.1 (4012216) (Important)	Microsoft XML Core Services 3.0 (4012216) (Important)	Adobe Flash Player (4014329) (Critical)
Windows 10								
Bulletin Identifier	**MS17-016**	**MS17-017**	**MS17-018**	**MS17-019**	**MS17-020**	**MS17-021**	**MS17-022**	**MS17-023**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**None**	**Important**	**Important**	**Critical**
Windows 10 for 32-bit Systems	Windows 10 for 32-bit Systems (4012606) (Important)	Windows 10 for 32-bit Systems (4012606) (Important)	Windows 10 for 32-bit Systems (4012606) (Important)	Not applicable	Not applicable	Windows 10 for 32-bit Systems (4012606) (Important)	Microsoft XML Core Services 3.0 (4012606) (Important)	Adobe Flash Player (4014329) (Critical)
Windows	Windows 10	Windows 10	Windows 10	Not applicable	Not applicable	Windows 10	Microsoft XML	Adobe Flash

10 for x64-based Systems	for x64-based Systems (4012606) (Important)	for x64-based Systems (4012606) (Important)	for x64-based Systems (4012606) (Important)			for x64-based Systems (4012606) (Important)	Core Services 3.0 (4012606) (Important)	Player (4014329) (Critical)
Windows 10 Version 1511 for 32-bit Systems	Windows 10 Version 1511 for 32-bit Systems (4013198) (Important)	Windows 10 Version 1511 for 32-bit Systems (4013198) (Important)	Windows 10 Version 1511 for 32-bit Systems (4013198) (Important)	Not applicable	Not applicable	Windows 10 Version 1511 for 32-bit Systems (4013198) (Important)	Microsoft XML Core Services 3.0 (4013198) (Important)	Adobe Flash Player (4014329) (Critical)
Windows 10 Version 1511 for x64-based Systems	Windows 10 Version 1511 for x64-based Systems (4013198) (Important)	Windows 10 Version 1511 for x64-based Systems (4013198) (Important)	Windows 10 Version 1511 for x64-based Systems (4013198) (Important)	Not applicable	Not applicable	Windows 10 Version 1511 for x64-based Systems (4013198) (Important)	Microsoft XML Core Services 3.0 (4013198) (Important)	Adobe Flash Player (4014329) (Critical)
Windows 10 Version 1607 for 32-bit Systems	Windows 10 Version 1607 for 32-bit Systems (4013429) (Important)	Windows 10 Version 1607 for 32-bit Systems (4013429) (Important)	Windows 10 Version 1607 for 32-bit Systems (4013429) (Important)	Not applicable	Not applicable	Windows 10 Version 1607 for 32-bit Systems (4013429) (Important)	Microsoft XML Core Services 3.0 (4013429) (Important)	Adobe Flash Player (4014329) (Critical)
Windows 10 Version 1607 for x64-based Systems	Windows 10 Version 1607 for x64-based Systems (4013429) (Important)	Windows 10 Version 1607 for x64-based Systems (4013429) (Important)	Windows 10 Version 1607 for x64-based Systems (4013429) (Important)	Not applicable	Not applicable	Windows 10 Version 1607 for x64-based Systems (4013429) (Important)	Microsoft XML Core Services 3.0 (4013429) (Important)	Adobe Flash Player (4014329) (Critical)
Windows 10 Version 1703 for 32-bit Systems	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Windows 10 Version 1703 for x64-based Systems	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Windows Server 2016								
Bulletin Identifier	**MS17-016**	**MS17-017**	**MS17-018**	**MS17-019**	**MS17-020**	**MS17-021**	**MS17-022**	**MS17-023**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Important**	**None**	**Important**	**Important**	**Critical**
Windows Server 2016 for x64-based Systems	Windows Server 2016 for x64-based Systems (4013429) (Important)	Windows Server 2016 for x64-based Systems (4013429) (Important)	Windows Server 2016 for x64-based Systems (4013429) (Important)	Windows Server 2016 for x64-based Systems (4013429) (Important)	Not applicable	Windows Server 2016 for x64-based Systems (4013429) (Important)	Microsoft XML Core Services 3.0 (4013429) (Important)	Adobe Flash Player (4014329) (Critical)
Server Core installation option								
Bulletin Identifier	**MS17-016**	**MS17-017**	**MS17-018**	**MS17-019**	**MS17-020**	**MS17-021**	**MS17-022**	**MS17-023**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Important**	**None**	**None**	**Important**	**None**
Windows	Windows	Windows	Windows	Not applicable	Not applicable	Not applicable	Microsoft XML	Not applicable

Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (4012373) (Important)	Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (4011981) (Important)	Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (4012497) (Important)				Core Services 3.0 (3216916) (Important)	
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (4012373) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (4011981) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (4012497) (Important)	Not applicable	Not applicable	Not applicable	Microsoft XML Core Services 3.0 (3216916) (Important)	Not applicable
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Security Only	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012212) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012212) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012212) (Important)	Not applicable	Not applicable	Not applicable	Microsoft XML Core Services 3.0 (4012212) (Important)	Not applicable
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Monthly Rollup	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012215) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012215) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (4012215) (Important)	Not applicable	Not applicable	Not applicable	Microsoft XML Core Services 3.0 (4012215) (Important)	Not applicable
Windows Server 2012 (Server Core installation) Security Only	Windows Server 2012 (Server Core installation) (4012214) (Important)	Windows Server 2012 (Server Core installation) (4012214) (Important)	Windows Server 2012 (Server Core installation) (4012214) (Important)	Windows Server 2012 (Server Core installation) (4012214) (Important)	Not applicable	Not applicable	Microsoft XML Core Services 3.0 (4012214) (Important)	Not applicable
Windows Server 2012 (Server Core installation) Monthly Rollup	Windows Server 2012 (Server Core installation) (4012217) (Important)	Windows Server 2012 (Server Core installation) (4012217) (Important)	Windows Server 2012 (Server Core installation) (4012217) (Important)	Windows Server 2012 (Server Core installation) (4012217) (Important)	Not applicable	Not applicable	Microsoft XML Core Services 3.0) (4012217) (Important)	Not applicable
Windows Server 2012 R2 (Server Core installation)	Windows Server 2012 R2 (Server Core installation) (4012213) (Important)	Windows Server 2012 R2 (Server Core installation) (4012213) (Important)	Windows Server 2012 R2 (Server Core installation) (4012213) (Important)	Windows Server 2012 R2 (Server Core installation) (4012213) (Important)	Not applicable	Not applicable	Microsoft XML Core Services 3.0 (4012213) (Important)	Not applicable

Security Only								
Windows Server 2012 R2 (Server Core installation) Monthly Rollup	Windows Server 2012 R2 (Server Core installation) (4012216) (Important)	Windows Server 2012 R2 (Server Core installation) (4012216) (Important)	Windows Server 2012 R2 (Server Core installation) (4012216) (Important)	Windows Server 2012 R2 (Server Core installation) (4012216) (Important)	Not applicable	Not applicable	Microsoft XML Core Services 3.0 (4012216) (Important)	Not applicable
Windows Server 2016 for x64-based Systems (Server Core installation)	Windows Server 2016 for x64-based Systems (Server Core installation) (4013429) (Important)	Windows Server 2016 for x64-based Systems (Server Core installation) (4013429) (Important)	Windows Server 2016 for x64-based Systems (Server Core installation) (4013429) (Important)	Windows Server 2016 for x64-based Systems (Server Core installation) (4013429) (Important)	Not applicable	Not applicable	Microsoft XML Core Services 3.0 (4013429) (Important)	Not applicable

Microsoft Office Suites and Software

Microsoft Office 2007		
Bulletin Identifier	**MS17-013**	**MS17-014**
Aggregate Severity Rating	**Critical**	**Important**
Microsoft Office 2007 Service Pack 3	Microsoft Office 2007 Service Pack 3 (3127945) (Critical) Microsoft Office 2007 Service Pack 3 (3141535) (Critical)	Microsoft Excel 2007 Service Pack 3 (3178676) (Important) Microsoft Word 2007 Service Pack 3 (3178683) (Important)
Microsoft Office 2010		
Bulletin Identifier	**MS17-013**	**MS17-014**
Aggregate Severity Rating	**Critical**	**Important**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3127958) (Critical) Microsoft Office 2010 Service Pack 2 (32-bit editions) (3178688) (Critical)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3178686) (Important) Microsoft Excel 2010 Service Pack 2 (32-bit editions) (3178690) (Important) Microsoft Word 2010 Service Pack 2 (32-bit editions) (3178687) (Important)
Microsoft Office 2010 Service Pack 2 (64-bit editions)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3127958) (Critical) Microsoft Office 2010 Service Pack 2 (64-bit editions) (3178688) (Critical)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3178686) (Important) Microsoft Excel 2010 Service Pack 2 (64-bit editions) (3178690) (Important)

		Microsoft Word 2010 Service Pack 2 (64-bit editions) (3178687) (Important)
Microsoft Office 2013		
Bulletin Identifier	**MS17-013**	**MS17-014**
Aggregate Severity Rating	**None**	**Important**
Microsoft Office 2013 Service Pack 1 (32-bit editions)	Not applicable	Microsoft Excel 2013 Service Pack 1 (32-bit editions) (3172542) (Important) Microsoft Word 2013 Service Pack 1 (32-bit editions) (3172464) (important)
Microsoft Office 2013 Service Pack 1 (64-bit editions)	Not applicable	Microsoft Excel 2013 Service Pack 1 (64-bit editions) (3172542) (Important) Microsoft Word 2013 Service Pack 1 (64-bit editions) (3172464) (important)
Microsoft Office 2013 RT		
Bulletin Identifier	**MS17-013**	**MS17-014**
Aggregate Severity Rating	**None**	**Important**
Microsoft Office 2013 RT Service Pack 1	Not applicable	Microsoft Excel 2013 RT Service Pack 1 (3172542) (Important) Microsoft Word 2013 RT Service Pack 1 (3172464) (important)
Microsoft Office 2016		
Bulletin Identifier	**MS17-013**	**MS17-014**
Aggregate Severity Rating	**None**	**Important**
Microsoft Office 2016 (32-bit edition)	Not applicable	Microsoft Excel 2016 (32-bit edition) (3178673) (Important) Microsoft Word 2016 (32-bit edition) (3178674) (Important)
Microsoft Office 2016 (64-bit edition)	Not applicable	Microsoft Excel 2016 (64-bit edition) (3178673) (Important) Microsoft Word 2016 (64-bit edition) (3178674) (Important)
Microsoft Office for Mac 2011		

Bulletin Identifier	MS17-013	MS17-014
Aggregate Severity Rating	**None**	**Important**
Microsoft Office for Mac 2011	Not applicable	Microsoft Excel for Mac 2011 (3198809) (Important) Microsoft Excel for Mac 2011 (3212218) (Important) Microsoft Word for Mac 2011 (3198809) (Important)
Microsoft Office 2016 for Mac		
Bulletin Identifier	**MS17-013**	**MS17-014**
Aggregate Severity Rating	**None**	**Important**
Microsoft Office 2016 for Mac	Not applicable	Microsoft Office 2016 for Mac (Important) Microsoft Excel 2016 for Mac (Important)
Other Office Software		
Bulletin Identifier	**MS17-013**	**MS17-014**
Aggregate Severity Rating	**Critical**	**Important**
Microsoft Office Compatibility Pack Service Pack 3	Not applicable	Microsoft Office Compatibility Pack Service Pack 3 (3178677) (Important) Microsoft Office Compatibility Pack Service Pack 3 (3178682) (Important)
Microsoft Excel Viewer	Not applicable	Microsoft Excel Viewer (3178680) (Important)
Microsoft Word Viewer	Microsoft Word Viewer (3178693) (Critical) Microsoft Word Viewer (3178653) (Critical)	Microsoft Word Viewer (3178694) (Important)

Note for MS17-013 and MS17-014

This bulletin spans more than one software category. See other tables in this section for additional affected software.

Microsoft Office Services and Web Apps

Microsoft SharePoint Server 2007	
Bulletin Identifier	**MS17-014**
Aggregate Severity Rating	**Important**

Microsoft SharePoint Server 2007 Service Pack 3	Excel Services (32-bit edition) (3178678) (Important)
Microsoft SharePoint Server 2007 Service Pack 3	Excel Services (64-bit edition) (3178678) (Important)
Microsoft SharePoint Server 2010	
Bulletin Identifier	**MS17-014**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2010 Service Pack 2	Excel Services (3178685) (Important) Word Automation Services (3178684) (Important)
Microsoft SharePoint Server 2013	
Bulletin Identifier	**MS17-014**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2013 Service Pack 1	Excel Services (3172431) (Important)
Microsoft Office Web Apps 2010	
Bulletin Identifier	**MS17-014**
Aggregate Severity Rating	**Important**
Microsoft Office Web Apps 2010 Service Pack 2	Microsoft Office Web Apps 2010 Service Pack 2 (3178689) (Important)
Microsoft Office Web Apps 2013	
Bulletin Identifier	**MS17-014**
Aggregate Severity Rating	**Important**
Microsoft Office Web Apps Server 2013 Service Pack 1	Microsoft Office Web Apps Server 2013 Service Pack 1 (3172457) (Important)

Note for MS17-014

This bulletin spans more than one software category. See other tables in this section for additional affected software.

Microsoft Server Software

Microsoft SharePoint Foundation 2013		
Bulletin Identifier	**MS17-014**	**MS17-015**
Aggregate Severity Rating	**Important**	**None**
Microsoft SharePoint Foundation 2013 Service	Microsoft SharePoint Foundation 2013 Service	Not applicable

Pack 1	Pack 1 (3172540) (Important)	
Microsoft Exchange Server 2013		
Bulletin Identifier	**MS17-014**	**MS17-015**
Aggregate Severity Rating	**None**	**Important**
Microsoft Exchange Server 2013 Service Pack 1	Not applicable	Microsoft Exchange Server 2013 Service Pack 1 (4012178) (Important)
Microsoft Exchange Server 2013 Cumulative Update 14	Not applicable	Microsoft Exchange Server 2013 Cumulative Update 14 (4012178) (Important)
Microsoft Exchange Server 2016		
Bulletin Identifier	**MS17-014**	**MS17-015**
Aggregate Severity Rating	**None**	**Important**
Microsoft Exchange Server 2016 Cumulative Update 3	Not applicable	Microsoft Exchange Server 2016 Cumulative Update 3 (4012178) (Important)

Note for MS17-014 and MS17-015

This bulletin spans more than one software category. See other tables in this section for additional affected software.

Microsoft Communications Platforms and Software

Skype for Business 2016		
Bulletin Identifier	**MS17-013**	**MS17-014**
Aggregate Severity Rating	**Critical**	**None**
Skype for Business 2016 (32-bit editions)	Skype for Business 2016 (32-bit editions) (3178656) (Critical)	Not applicable
Skype for Business Basic 2016 (32-bit editions)	Skype for Business Basic 2016 (32-bit editions) (3178656) (Critical)	Not applicable
Skype for Business 2016 (64-bit editions)	Skype for Business 2016 (64-bit editions) (3178656) (Critical)	Not applicable
Skype for Business Basic 2016 (64-bit editions)	Skype for Business Basic 2016 (64-bit editions) (3178656) (Critical)	Not applicable
Microsoft Lync 2013		
Bulletin Identifier	**MS17-013**	**MS17-014**
Aggregate Severity Rating	**Critical**	**None**
Microsoft Lync 2013 Service Pack 1 (32-bit) (Skype for Business)	Microsoft Lync 2013 Service Pack 1 (32-bit) (Skype for Business)	Not applicable

	(3172539) (Critical)	
Microsoft Lync Basic 2013 Service Pack 1 (32-bit) (Skype for Business Basic)	Microsoft Lync Basic 2013 Service Pack 1 (32-bit) (Skype for Business Basic) (3172539) (Critical)	Not applicable
Microsoft Lync 2013 Service Pack 1 (64-bit) (Skype for Business)	Microsoft Lync 2013 Service Pack 1 (64-bit) (Skype for Business) (3172539) (Critical)	Not applicable
Microsoft Lync Basic 2013 Service Pack 1 (64-bit) (Skype for Business Basic)	Microsoft Lync Basic 2013 Service Pack 1 (64-bit) (Skype for Business Basic) (3172539) (Critical)	Not applicable
Microsoft Lync 2010		
Bulletin Identifier	**MS17-013**	**MS17-014**
Aggregate Severity Rating	**Critical**	**None**
Microsoft Lync 2010 (32-bit)	Microsoft Lync 2010 (32-bit) (4010299) (Critical)	Not applicable
Microsoft Lync 2010 (64-bit)	Microsoft Lync 2010 (64-bit) (4010299) (Critical)	Not applicable
Microsoft Lync 2010 Attendee (user level install)	Microsoft Lync 2010 Attendee (user level install) (4010300) (Critical)	Not applicable
Microsoft Lync 2010 Attendee (admin level install)	Microsoft Lync 2010 Attendee (admin level install) (4010301) (Critical)	Not applicable
Microsoft Live Meeting 2007 Console		
Bulletin Identifier	**MS17-013**	**MS17-014**
Aggregate Severity Rating	**Critical**	**None**
Microsoft Live Meeting 2007 Console	Microsoft Live Meeting 2007 Console (4010303) (Critical)	Not applicable
Microsoft Live Meeting 2007 Add-in		
Bulletin Identifier	**MS17-013**	**MS17-014**
Aggregate Severity Rating	**Critical**	**None**
Microsoft Live Meeting 2007 Add-in	Microsoft Live Meeting 2007 Add-in (4010304) (Critical)	Not applicable
Microsoft Lync for Mac		
Bulletin Identifier	**MS17-013**	**MS17-014**
Aggregate Severity Rating	**None**	**Important**
Microsoft Lync for Mac 2011	Not applicable	Microsoft Lync for Mac 2011

		(4012487) (Important)

Note for MS17-013 and MS17-014

This bulletin spans more than one software category. See other tables in this section for additional affected software.

Microsoft Developer Tools and Software

Microsoft Silverlight	
Bulletin Identifier	**MS17-013**
Aggregate Severity Rating	**Critical**
Microsoft Silverlight 5 when installed on all supported releases of Microsoft Windows clients	Microsoft Silverlight 5 when installed on all supported releases of Microsoft Windows clients (4013867) **(**Critical)
Microsoft Silverlight 5 Developer Runtime when installed on all supported releases of Microsoft Windows clients	Microsoft Silverlight 5 Developer Runtime when installed on all supported releases of Microsoft Windows clients (4013867) **(**Critical)
Microsoft Silverlight 5 when installed on all supported releases of Microsoft Windows servers	Microsoft Silverlight 5 when installed on all supported releases of Microsoft Windows servers (4013867) **(**Critical)
Microsoft Silverlight 5 Developer Runtime when installed on all supported releases of Microsoft Windows servers	Microsoft Silverlight 5 Developer Runtime when installed on all supported releases of Microsoft Windows servers (4013867) **(**Critical)

Note for MS17-013

This bulletin spans more than one software category. See other tables in this section for additional affected software.

Detection and Deployment Tools and Guidance

Several resources are available to help administrators deploy security updates.

Microsoft Baseline Security Analyzer (MBSA) lets administrators scan local and remote systems for missing security updates and common security misconfigurations.

Windows Server Update Services (WSUS), Systems Management Server (SMS), and System Center Configuration Manager help administrators distribute security updates.

The Update Compatibility Evaluator components included with Application Compatibility Toolkit aid in streamlining the testing and validation of Windows updates against installed applications.

For information about these and other tools that are available, see Security Tools for IT Pros.

Acknowledgments

Microsoft recognizes the efforts of those in the security community who help us protect customers through responsible vulnerability disclosure. See Acknowledgments for more information.

Other Information

Microsoft Windows Malicious Software Removal Tool

For the bulletin release that occurs on the second Tuesday of each month, Microsoft has released an updated version of the Microsoft Windows Malicious Software Removal Tool on Windows Update, Microsoft Update, Windows Server Update Services, and the Download Center. No updated version of the Microsoft Windows Malicious Software Removal Tool is available for out-of-band security bulletin releases.

Non-Security Updates on MU, WU, and WSUS

For information about non-security releases on Windows Update and Microsoft Update, please see:

- Microsoft Knowledge Base Article 894199: Description of Software Update Services and Windows Server Update Services changes in content. Includes all Windows content.
- Updates from Past Months for Windows Server Update Services. Displays all new, revised, and rereleased updates for Microsoft products other than Microsoft Windows.

Microsoft Active Protections Program (MAPP)

To improve security protections for customers, Microsoft provides vulnerability information to major security software providers in advance of each monthly security update release. Security software providers can then use this vulnerability information to provide updated protections to customers via their security software or devices, such as antivirus, network-based intrusion detection systems, or host-based intrusion prevention systems. To determine whether active protections are available from security software providers, please visit the active protections websites provided by program partners listed in Microsoft Active Protections Program (MAPP) Partners.

Security Strategies and Community

Update Management Strategies

Security Guidance for Update Management provides additional information about Microsoft's best-practice recommendations for applying security updates.

Obtaining Other Security Updates

Updates for other security issues are available from the following locations:

- Security updates are available from Microsoft Download Center. You can find them most easily by doing a keyword search for "security update".
- Updates for consumer platforms are available from Microsoft Update.
- You can obtain the security updates offered this month on Windows Update, from Download Center on Security and Critical Releases ISO CD Image files. For more information, see Microsoft Knowledge Base Article 913086.

IT Pro Security Community

Learn to improve security and optimize your IT infrastructure, and participate with other IT Pros on security topics in IT Pro Security Community.

Support

The affected software listed has been tested to determine which versions are affected. Other versions are past their support life cycle. To determine the support life cycle for your software version, visit Microsoft Support Lifecycle.

Security solutions for IT professionals: TechNet Security Troubleshooting and Support

Help protect your computer that is running Windows from viruses and malware: Virus Solution and Security Center

Local support according to your country: International Support

Disclaimer

The information provided in the Microsoft Knowledge Base is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions

- V1.0 (March 14, 2017): Bulletin Summary published.
- V2.0 (April 11, 2017): Bulletin Summary revised to announce the following updates:
  - For MS17-013, the release of update 4017018 for Windows Vista and Windows Server 2008. The update replaces update 4012583 for CVE-2017-0038 only, to comprehensively address the vulnerability. Microsoft recommends that customers running the affected software install the security update to be fully protected from the vulnerability described in this bulletin. See Microsoft Knowledge Base Article 4017018 for more information.
  - For MS17-014, to comprehensively address CVE-2017-0027 for Office for Mac 2011 only, Microsoft is releasing security update 3212218. Microsoft recommends that customers running Office for Mac 2011 install update 3212218 to be fully protected from this vulnerability. See Microsoft Knowledge Base Article 3212218 for more information.
  - For MS17-021, security updates that apply to CVE-2017-0042 for Windows Server 2012 are now available. Customers running Windows Server 2012 should install update 4015548 (Security Only) or 4015551 (Monthly Rollup) to be fully protected from this vulnerability. Customers running other versions of Microsoft Windows do not need to take any further action.
- V2.1 (April 14, 2017) CVE-2017-0022 revised to update the Exploitability Index to 0 - Exploitation Detected. This is an informational change only.

- V3.0 (May 9, 2017): For MS17-013, Microsoft has re-released security update 4017018 for affected editions of Windows Server 2008. The re-release has been re-classified as a security update. Microsoft recommends that customers should install update 4017018 to be fully protected from CVE-2017-0038. Customers who have already installed the update do not need to take any further action.
- V4.0 (August 8, 2017): For MS17-007, to comprehensively address CVE-2017-0071, Microsoft released the July security updates for all versions of Windows 10. Note that Windows 10 for 32-bit Systems, Windows 10 for x64-based Systems, Windows 10 Version 1703 for 32-bit Systems, and Windows 10 Version 1703 for x64-based Systems have been added to the Affected Products table as they are also affected by this vulnerability. Microsoft recommends that customers who have not already done so install the July 2017 security updates to be fully protected from this vulnerability.

Page generated 2017-08-02 12:34-07:00.

© 2017 Microsoft