Microsoft Security Bulletin Summary for February 2016

Published: February 9, 2016 | Updated: February 24, 2016

Version: 3.1

This bulletin summary lists security bulletins released for February 2016.

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**.

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
MS16-009	**Cumulative Security Update for Internet Explorer (3134220)** 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 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 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	3134814	Microsoft Windows, Internet Explorer
MS16-011	**Cumulative Security Update for Microsoft Edge (3134225)** This security update resolves vulnerabilities in Microsoft Edge. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Microsoft Edge. An attacker who successfully exploited the vulnerabilities could gain the same user rights as 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.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows, Microsoft Edge
MS16-012	**Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (3138938)** This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code	Critical Remote Code Execution	May require restart	---------	Microsoft Windows

	execution if Microsoft Windows PDF Library improperly handles application programming interface (API) calls, which could allow an attacker to run arbitrary code on the user's system. An attacker who successfully exploited the vulnerabilities could gain the same user rights as 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. However, an attacker would have no way to force users to download or open a malicious PDF document.				
MS16-013	**Security Update for Windows Journal to Address Remote Code Execution (3134811)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted Journal file. 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	May require restart	---------	Microsoft Windows
MS16-014	**Security Update for Microsoft Windows to Address Remote Code Execution (3134228)** This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.	Important Remote Code Execution	Requires restart	3126041 3126587 3126593	Microsoft Windows
MS16-015	**Security Update for Microsoft Office to Address Remote Code Execution (3134226)** 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.	Critical Remote Code Execution	May require restart	---------	Microsoft Office, Microsoft Office Services and Web Apps, Microsoft Server Software
MS16-016	**Security Update for WebDAV to Address Elevation of Privilege (3136041)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker uses the Microsoft Web Distributed Authoring and Versioning (WebDAV) client to send specifically crafted input to a server.	Important Elevation of Privilege	May require restart	---------	Microsoft Windows
MS16-017	**Security Update for Remote Desktop Display Driver to Address Elevation of Privilege (3134700)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an authenticated attacker logs on to the target system using RDP and sends specially crafted data over the connection. By default, RDP is not enabled on any Windows operating system. Systems that do not have RDP enabled are not at risk.	Important Elevation of Privilege	Requires restart	3134700 3126446	Microsoft Windows

MS16-018	**Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3136082)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application.	Important Elevation of Privilege	Requires restart	---------	Microsoft Windows
MS16-019	**Security Update for .NET Framework to Address Denial of Service (3137893)** This security update resolves vulnerabilities in Microsoft .NET Framework. The more severe of the vulnerabilities could cause denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part, causing the server to recursively compile XSLT transforms.	Important Denial of Service	May require restart	---------	Microsoft Windows, Microsoft .NET Framework
MS16-020	**Security Update for Active Directory Federation Services to Address Denial of Service (3134222)** This security update resolves a vulnerability in Active Directory Federation Services (ADFS). The vulnerability could allow denial of service if an attacker sends certain input data during forms-based authentication to an ADFS server, causing the server to become nonresponsive.	Important Denial of Service	May require restart	---------	Microsoft Windows
MS16-021	**Security Update for NPS RADIUS Server to Address Denial of Service (3133043)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could cause denial of service on a Network Policy Server (NPS) if an attacker sends specially crafted username strings to the NPS, which could prevent RADIUS authentication on the NPS.	Important Denial of Service	May require restart	---------	Microsoft Windows
MS16-022	**Security Update for Adobe Flash Player (3135782)** This security update resolves vulnerabilities in Adobe Flash Player when installed on all supported editions of Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, and Windows 10.	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

MS16-009: Cumulative Security Update for Internet Explorer (3134220)				
CVE-2016-0041	DLL Loading Remote Code Execution Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0059	Internet Explorer Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-0060	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0061	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0062	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0063	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0064	Internet Explorer Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2016-0067	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0068	Internet Explorer Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0069	Internet Explorer Elevation of Privilege Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
CVE-2016-0071	Internet Explorer Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2016-0072	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0077	Microsoft Browser Spoofing Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS16-011: Cumulative Security Update for Microsoft Edge (3134225)				
CVE-2016-0060	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-0061	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-0062	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable

CVE-2016-0077	Microsoft Browser Spoofing Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-0080	Microsoft Edge ASLR Bypass	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-0084	Microsoft Edge Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
MS16-012: Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (3138938)				
CVE-2016-0046	Microsoft Windows Reader Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-0058	Microsoft PDF Library Buffer Overflow Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
MS16-013: Security Update for Windows Journal to Address Remote Code Execution (3134811)				
CVE-2016-0038	Windows Journal Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution (3134228)				
CVE-2016-0040	Windows Elevation of Privilege Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-0041	DLL Loading Remote Code Execution Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
CVE-2016-0042	Windows DLL Loading Remote Code Execution Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0044	Windows DLL Loading Denial of Service Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Permanent
CVE-2016-0049	Windows Kerberos Security Feature Bypass	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-015: Security Update for Microsoft Office to Address Remote Code Execution (3134226)				
CVE-2016-0022	Microsoft Office Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0039	Microsoft SharePoint XSS Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
CVE-2016-0052	Microsoft Office Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0053	Microsoft Office Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0054	Microsoft Office Memory Corruption	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable

	Vulnerability			
CVE-2016-0055	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2016-0056	Microsoft Office Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
MS16-016: Security Update for WebDAV to Address Elevation of Privilege (3136041)				
CVE-2016-0051	WebDAV Elevation of Privilege Vulnerability	3 - Exploitation Unlikely	2 - Exploitation Less Likely	Not applicable
MS16-017: Security Update for Remote Desktop Display Driver to Address Elevation of Privilege (3134700)				
CVE-2016-0036	Remote Desktop Protocol (RDP) Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-018: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3136082)				
CVE-2016-0048	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Permanent
MS16-019: Security Update for .NET Framework to Address Denial of Service (3137893)				
CVE-2016-0033	.NET Framework Stack Overflow Denial of Service Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Permanent
CVE-2016-0047	Windows Forms Information Disclosure Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-020: Security Update for Active Directory Federation Services to Address Denial of Service (3134222)				
CVE-2016-0037	Microsoft Active Directory Federation Services Denial of Service Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Permanent
MS16-021: Security Update for NPS RADIUS Server to Address Denial of Service (3133043)				
CVE-2016-0050	Network Policy Server RADIUS Implementation Denial of Service Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Permanent
MS16-022: Security Update for Adobe Flash Player (3135782)				
APSB16-04	See Adobe Security Bulletin APSB16-04 for vulnerability severity and update priority ratings.	Not applicable	Not applicable	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	**MS16-009**	**MS16-011**	**MS16-012**	**MS16-013**	**MS16-014**	**MS16-016**
Aggregate Severity Rating	**Critical**	**None**	**None**	**Critical**	**Important**	**Important**
Windows Vista Service Pack 2	Internet Explorer 9 (3134814) (Critical)	Not applicable	Not applicable	Windows Vista Service Pack 2 (3115858) (Critical)	Windows Vista Service Pack 2 (3126587) (Important) Windows Vista Service Pack 2 (3126593) (Important) Windows Vista Service Pack 2 (3126041) (Important)	Windows Vista Service Pack 2 (3124280) (Important)
Windows Vista x64 Edition Service Pack 2	Internet Explorer 9 (3134814) (Critical)	Not applicable	Not applicable	Windows Vista x64 Edition Service Pack 2 (3115858) (Critical)	Windows Vista x64 Edition Service Pack 2 (3126587) (Important) Windows Vista x64 Edition Service Pack 2 (3126593) (Important) Windows Vista x64 Edition Service Pack 2 (3126041) (Important)	Windows Vista x64 Edition Service Pack 2 (3124280) (Important)
Windows Server 2008						
Bulletin Identifier	**MS16-009**	**MS16-011**	**MS16-012**	**MS16-013**	**MS16-014**	**MS16-016**

Aggregate Severity Rating	**Moderate**	**None**	**None**	**Critical**	**Important**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2	Internet Explorer 9 (3134814) (Moderate)	Not applicable	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3115858) (Critical)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3126587) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (3126593) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (3126041) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3124280) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Internet Explorer 9 (3134814) (Moderate)	Not applicable	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3115858) (Critical)	Windows Server 2008 for x64-based Systems Service Pack 2 (3126587) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (3126593) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (3126041) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (3124280) (Important)
Windows Server 2008 for Itanium-based Systems Service Pack 2	Internet Explorer 9 (3134814) (Moderate)	Not applicable	Not applicable	Not applicable	Windows Server 2008 for Itanium-based Systems	Not applicable

					Service Pack 2 (3126587) (Important) Windows Server 2008 for Itanium-based Systems Service Pack 2 (3126593) (Important) Windows Server 2008 for Itanium-based Systems Service Pack 2 (3126041) (Important)	
Windows 7						
Bulletin Identifier	**MS16-009**	**MS16-011**	**MS16-012**	**MS16-013**	**MS16-014**	**MS16-016**
Aggregate Severity Rating	**Critical**	**None**	**None**	**Critical**	**Important**	**Important**
Windows 7 for 32-bit Systems Service Pack 1	Internet Explorer 11 (3134814) (Critical)	Not applicable	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3115858) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3126587) (Important) Windows 7 for 32-bit Systems Service Pack 1 (3126593) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3124280) (Important)
Windows 7 for x64-based Systems Service Pack 1	Internet Explorer 11 (3134814) (Critical)	Not applicable	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3115858) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3126587) (Important) Windows 7 for x64-based Systems Service Pack 1 (3126593) (Important)	Windows 7 for x64-based Systems Service Pack 1 (3124280) (Important)

Windows Server 2008 R2						
Bulletin Identifier	**MS16-009**	**MS16-011**	**MS16-012**	**MS16-013**	**MS16-014**	**MS16-016**
Aggregate Severity Rating	**Moderate**	**None**	**None**	**Critical**	**Important**	**Important**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Internet Explorer 11 (3134814) (Moderate)	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3115858) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3126587) (Important) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3126593) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3124280) (Important)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Internet Explorer 11 (3134814) (Moderate)	Not applicable	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3126587) (Important) Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3126593) (Important)	Not applicable
Windows 8.1						
Bulletin Identifier	**MS16-009**	**MS16-011**	**MS16-012**	**MS16-013**	**MS16-014**	**MS16-016**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**Important**	**Moderate**
Windows 8.1 for 32-bit Systems	Internet Explorer 11 (3134814) (Critical)	Not applicable	Windows 8.1 for 32-bit Systems (3123294) (Critical)	Windows 8.1 for 32-bit Systems (3115858) (Critical)	Windows 8.1 for 32-bit Systems (3126587) (Important) Windows 8.1 for 32-bit Systems (3126593) (Important)	Windows 8.1 for 32-bit Systems (3124280) (Moderate)

					Windows 8.1 for 32-bit Systems (3126041) (Important) Windows 8.1 for 32-bit Systems (3126434) (Important)	
Windows 8.1 for x64-based Systems	Internet Explorer 11 (3134814) (Critical)	Not applicable	Windows 8.1 for x64-based Systems (3123294) (Critical)	Windows 8.1 for x64-based Systems (3115858) (Critical)	Windows 8.1 for x64-based Systems (3126587) (Important) Windows 8.1 for x64-based Systems (3126593) (Important) Windows 8.1 for x64-based Systems (3126041) (Important) Windows 8.1 for x64-based Systems (3126434) (Important)	Windows 8.1 for x64-based Systems (3124280) (Moderate)
Windows Server 2012 and Windows Server 2012 R2						
Bulletin Identifier	**MS16-009**	**MS16-011**	**MS16-012**	**MS16-013**	**MS16-014**	**MS16-016**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**Critical**	**Important**	**Moderate**
Windows Server 2012	Internet Explorer 10 (3134814) (Moderate)	Not applicable	Windows Server 2012 (3123294) (Critical)	Windows Server 2012 (3115858) (Critical)	Windows Server 2012 (3126587) (Important) Windows Server 2012 (3126593) (Important)	Windows Server 2012 (3124280) (Moderate)
Windows Server 2012 R2	Internet Explorer 11 (3134814) (Moderate)	Not applicable	Windows Server 2012 R2 (3123294) (Critical)	Windows Server 2012 R2 (3115858) (Critical)	Windows Server 2012 R2 (3126587) (Important) Windows Server	Windows Server 2012 R2 (3124280) (Moderate)

					2012 R2 (3126593) (Important) Windows Server 2012 R2 (3126041) (Important) Windows Server 2012 R2 (3126434) (Important)	
Windows RT 8.1						
Bulletin Identifier	**MS16-009**	**MS16-011**	**MS16-012**	**MS16-013**	**MS16-014**	**MS16-016**
Aggregate Severity Rating	**Critical**	**None**	**None**	**None**	**Important**	**Moderate**
Windows RT 8.1	Internet Explorer 11 (3134814) (Critical)	Not applicable	Not applicable	Not applicable	Windows RT 8.1 (3126587) (Important) Windows RT 8.1 (3126593) (Important) Windows RT 8.1 (3126434) (Important)	Windows RT 8.1 (3124280) (Moderate)
Windows 10						
Bulletin Identifier	**MS16-009**	**MS16-011**	**MS16-012**	**MS16-013**	**MS16-014**	**MS16-016**
Aggregate Severity Rating	**Critical**	**Critical**	**Critical**	**Critical**	**Important**	**Moderate**
Windows 10 for 32-bit Systems	Internet Explorer 11 (3135174) (Critical)	Microsoft Edge (3135174) (Critical)	Windows 10 for 32-bit Systems (3135174) (Critical)	Windows 10 for 32-bit Systems (3135174) (Critical)	Windows 10 for 32-bit Systems (3135174) (Important)	Windows 10 for 32-bit Systems (3135174) (Moderate)
Windows 10 for x64-based Systems	Internet Explorer 11 (3135174) (Critical)	Microsoft Edge (3135174) (Critical)	Windows 10 for x64-based Systems (3135174) (Critical)	Windows 10 for x64-based Systems (3135174) (Critical)	Windows 10 for x64-based Systems (3135174) (Important)	Windows 10 for x64-based Systems (3135174) (Moderate)
Windows 10 Version 1511 for 32-bit Systems	Internet Explorer 11 (3135173) (Critical)	Microsoft Edge (3135173) (Critical)	Not applicable	Windows 10 Version 1511 for 32-bit Systems (3135173) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3135173) (Important)	Windows 10 Version 1511 for 32-bit Systems (3135173) (Moderate)
Windows 10 Version 1511 for x64-based	Internet	Microsoft	Not applicable	Windows 10	Windows	Windows 10

Systems	Explorer 11 (3135173) (Critical)	Edge (3135173) (Critical)		Version 1511 for x64-based Systems (3135173) (Critical)	10 Version 1511 for x64-based Systems (3135173) (Important)	Version 1511 for x64-based Systems (3135173) (Moderate)
Server Core installation option						
Bulletin Identifier	**MS16-009**	**MS16-011**	**MS16-012**	**MS16-013**	**MS16-014**	**MS16-016**
Aggregate Severity Rating	**None**	**None**	**Critical**	**None**	**Important**	**None**
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) (3126587) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3126593) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3126041) (Important)	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	Not applicable	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3126587) (Important) Windows Server	Not applicable

					2008 for x64-based Systems Service Pack 2 (Server Core installation) (3126593) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3126041) (Important)	
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Not applicable	Not applicable	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3126587) (Important) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3126593) (Important)	Not applicable
Windows Server 2012 (Server Core installation)	Not applicable	Not applicable	Not applicable	Not applicable	Windows Server 2012 (Server Core installation) (3126587) (Important) Windows Server 2012 (Server Core installation) (3126593) (Important)	Not applicable

Windows Server 2012 R2 (Server Core installation)	Not applicable	Not applicable	Windows Server 2012 R2 (Server Core installation) (3123294) (Critical)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3126587) (Important) Windows Server 2012 R2 (Server Core installation) (3126593) (Important) Windows Server 2012 R2 (Server Core installation) (3126041) (Important)	Not applicable

Windows Operating Systems and Components (Table 2 of 2)

Windows Vista						
Bulletin Identifier	**MS16-017**	**MS16-018**	**MS16-019**	**MS16-020**	**MS16-021**	**MS16-022**
Aggregate Severity Rating	**None**	**Important**	**Important**	**None**	**None**	**None**
Windows Vista Service Pack 2	Not applicable	Windows Vista Service Pack 2 (3134214) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (3122646) (Important) Microsoft .NET Framework 2.0 Service Pack 2 (3127219) (Important) Microsoft .NET Framework 4.5.2 (3122656) (Important) Microsoft .NET Framework 4.5.2 (3127229) (Important) Microsoft .NET Framework 4.6 (3122661) (Important)	Not applicable	Not applicable	Not applicable

			Microsoft .NET Framework 4.6 (3127233) (Important)			
Windows Vista x64 Edition Service Pack 2	Not applicable	Windows Vista x64 Edition Service Pack 2 (3134214) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (3122646) (Important) Microsoft .NET Framework 2.0 Service Pack 2 (3127219) (Important) Microsoft .NET Framework 4.5.2 (3122656) (Important) Microsoft .NET Framework 4.5.2 (3127229) (Important) Microsoft .NET Framework 4.6 (3122661) (Important) Microsoft .NET Framework 4.6 (3127233) (Important)	Not applicable	Not applicable	Not applicable
Windows Server 2008						
Bulletin Identifier	**MS16-017**	**MS16-018**	**MS16-019**	**MS16-020**	**MS16-021**	**MS16-022**
Aggregate Severity Rating	**None**	**Important**	**Important**	**None**	**Important**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3134214) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (3122646) (Important) Microsoft .NET Framework 2.0 Service Pack 2 (3127219) (Important) Microsoft .NET Framework 4.5.2 (3122656) (Important) Microsoft .NET Framework 4.5.2	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3133043) (Important)	Not applicable

			(3127229) (Important) Microsoft .NET Framework 4.6 (3122661) (Important) Microsoft .NET Framework 4.6 (3127233) (Important)			
Windows Server 2008 for x64-based Systems Service Pack 2	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3134214) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (3122646) (Important) Microsoft .NET Framework 2.0 Service Pack 2 (3127219) (Important) Microsoft .NET Framework 4.5.2 (3122656) (Important) Microsoft .NET Framework 4.5.2 (3127229) (Important) Microsoft .NET Framework 4.6 (3122661) (Important) Microsoft .NET Framework 4.6 (3127233) (Important)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3133043) (Important)	Not applicable
Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3134214) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (3122646) (Important) Microsoft .NET Framework 2.0 Service Pack 2 (3127219) (Important)	Not applicable	Not applicable	Not applicable
Windows 7						
Bulletin Identifier	**MS16-017**	**MS16-018**	**MS16-019**	**MS16-020**	**MS16-021**	**MS16-022**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**None**	**None**
Windows 7 for 32-bit Systems Service	Windows 7 for 32-bit Systems	Windows 7 for 32-bit Systems Service Pack	Microsoft .NET Framework	Not applicable	Not applicable	Not applicable

Pack 1	Service Pack 1 (3126446) (Important)	1 (3134214) (Important)	3.5.1 (3122648) (Important) Microsoft .NET Framework 3.5.1 (3127220) (Important) Microsoft .NET Framework 4.5.2 (3122656) (Important) Microsoft .NET Framework 4.5.2 (3127229) (Important) Microsoft .NET Framework 4.6/4.6.1 (3122661) (Important) Microsoft .NET Framework 4.6/4.6.1 (3127233) (Important)			
Windows 7 for x64-based Systems Service Pack 1	Windows 7 for x64-based Systems Service Pack 1 (3126446) (Important)	Windows 7 for x64-based Systems Service Pack 1 (3134214) (Important)	Microsoft .NET Framework 3.5.1 (3122648) (Important) Microsoft .NET Framework 3.5.1 (3127220) (Important) Microsoft .NET Framework 4.5.2 (3122656) (Important) Microsoft .NET Framework 4.5.2 (3127229) (Important) Microsoft .NET Framework 4.6/4.6.1 (3122661) (Important) Microsoft .NET Framework 4.6/4.6.1 (3127233) (Important)	Not applicable	Not applicable	Not applicable

Windows Server 2008 R2						
Bulletin Identifier	**MS16-017**	**MS16-018**	**MS16-019**	**MS16-020**	**MS16-021**	**MS16-022**
Aggregate Severity Rating	**None**	**Important**	**Important**	**None**	**Important**	**None**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3134214) (Important)	Microsoft .NET Framework 3.5.1 (3122648) (Important) Microsoft .NET Framework 3.5.1 (3127220) (Important) Microsoft .NET Framework 4.5.2 (3122656) (Important) Microsoft .NET Framework 4.5.2 (3127229) (Important) Microsoft .NET Framework 4.6/4.6.1 (3122661) (Important) Microsoft .NET Framework 4.6/4.6.1 (3127233) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3133043) (Important)	Not applicable
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3134214) (Important)	Microsoft .NET Framework 3.5.1 (3122648) (Important) Microsoft .NET Framework 3.5.1 (3127220) (Important)	Not applicable	Not applicable	Not applicable
Windows 8.1						
Bulletin Identifier	**MS16-017**	**MS16-018**	**MS16-019**	**MS16-020**	**MS16-021**	**MS16-022**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**None**	**Critical**
Windows 8.1 for 32-bit Systems	Windows 8.1 for 32-bit Systems (3126446) (Important)	Windows 8.1 for 32-bit Systems (3134214) (Important)	Microsoft .NET Framework 3.5 (3122651) (Important)	Not applicable	Not applicable	Adobe Flash Player (3135782) (Critical)

			Microsoft .NET Framework 3.5 (3127222) (Important) Microsoft .NET Framework 4.5.2 (3122654) (Important) Microsoft .NET Framework 4.5.2 (3127226) (Important) Microsoft .NET Framework 4.6/4.6.1 (3122660) (Important) Microsoft .NET Framework 4.6/4.6.1 (3127231) (Important)			
Windows 8.1 for x64-based Systems	Windows 8.1 for x64-based Systems (3126446) (Important)	Windows 8.1 for x64-based Systems (3134214) (Important)	Microsoft .NET Framework 3.5 (3122651) (Important) Microsoft .NET Framework 3.5 (3127222) (Important) Microsoft .NET Framework 4.5.2 (3122654) (Important) Microsoft .NET Framework 4.5.2 (3127226) (Important) Microsoft .NET Framework 4.6/4.6.1 (3122660) (Important) Microsoft .NET Framework 4.6/4.6.1 (3127231) (Important)	Not applicable	Not applicable	Adobe Flash Player (3135782) (Critical)
Windows Server 2012 and Windows Server 2012 R2						
Bulletin Identifier	**MS16-017**	**MS16-018**	**MS16-019**	**MS16-020**	**MS16-021**	**MS16-022**

Aggregate Severity Rating	**Important**	**Important**	**Important**	**Important**	**Important**	**Critical**
Windows Server 2012	Windows Server 2012 (3126446) (Important)	Windows Server 2012 (3134214) (Important)	Microsoft .NET Framework 3.5 (3122649) (Important) Microsoft .NET Framework 3.5 (3127221) (Important) Microsoft .NET Framework 4.5.2 (3122655) (Important) Microsoft .NET Framework 4.5.2 (3127227) (Important) Microsoft .NET Framework 4.6/4.6.1 (3122658) (Important) Microsoft .NET Framework 4.6/4.6.1 (3127230) (Important)	Not applicable	Windows Server 2012 (3133043) (Important)	Adobe Flash Player (3135782) (Critical)
Windows Server 2012 R2	Windows Server 2012 R2 (3126446) (Important)	Windows Server 2012 R2 (3134214) (Important)	Microsoft .NET Framework 3.5 (3122651) (Important) Microsoft .NET Framework 3.5 (3127222) (Important) Microsoft .NET Framework 4.5.2 (3122654) (Important) Microsoft .NET Framework 4.5.2 (3127226) (Important) Microsoft .NET Framework 4.6/4.6.1 (3122660) (Important) Microsoft .NET Framework 4.6/4.6.1	Active Directory Federation Services 3.0 (3134222) (Important)	Windows Server 2012 R2 (3133043) (Important)	Adobe Flash Player (3135782) (Critical)

			(3127231) (Important)			
Windows RT 8.1						
Bulletin Identifier	**MS16-017**	**MS16-018**	**MS16-019**	**MS16-020**	**MS16-021**	**MS16-022**
Aggregate Severity Rating	**None**	**Important**	**Important**	**None**	**None**	**Critical**
Windows RT 8.1	Not applicable	Windows RT 8.1 (3134214) (Important)	Microsoft .NET Framework 4.5.2 (3122654) (Important) Microsoft .NET Framework 4.5.2 (3127226) (Important) Microsoft .NET Framework 4.6/4.6.1 (3122660) (Important) Microsoft .NET Framework 4.6/4.6.1 (3127231) (Important)	Not applicable	Not applicable	Adobe Flash Player (3135782) (Critical)
Windows 10						
Bulletin Identifier	**MS16-017**	**MS16-018**	**MS16-019**	**MS16-020**	**MS16-021**	**MS16-022**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**None**	**None**	**Critical**
Windows 10 for 32-bit Systems	Windows 10 for 32-bit Systems (3135174) (Important)	Windows 10 for 32-bit Systems (3135174) (Important)	Microsoft .NET Framework 3.5 (3135174) (Important) Microsoft .NET Framework 4.6 (3135174) (Important)	Not applicable	Not applicable	Adobe Flash Player (3135782) (Critical)
Windows 10 for x64-based Systems	Windows 10 for x64-based Systems (3135174) (Important)	Windows 10 for x64-based Systems (3135174) (Important)	Microsoft .NET Framework 3.5 (3135174) (Important) Microsoft .NET Framework 4.6 (3135174) (Important)	Not applicable	Not applicable	Adobe Flash Player (3135782) (Critical)
Windows 10 Version 1511 for 32-bit Systems	Not applicable	Windows 10 Version 1511 for 32-bit Systems (3135173) (Important)	Microsoft .NET Framework 3.5 (3135173) (Important) Microsoft .NET	Not applicable	Not applicable	Adobe Flash Player (3135782) (Critical)

			Framework 4.6.1 (3135173) (Important)			
Windows 10 Version 1511 for x64-based Systems	Not applicable	Windows 10 Version 1511 for x64-based Systems (3135173) (Important)	Microsoft .NET Framework 3.5 (3135173) (Important) Microsoft .NET Framework 4.6.1 (3135173) (Important)	Not applicable	Not applicable	Adobe Flash Player (3135782) (Critical)
Server Core installation option						
Bulletin Identifier	**MS16-017**	**MS16-018**	**MS16-019**	**MS16-020**	**MS16-021**	**MS16-022**
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Important**	**Important**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3134214) (Important)	Not applicable	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3133043) (Important)	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3134214) (Important)	Not applicable	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3133043) (Important)	Not applicable
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3134214) (Important)	Microsoft .NET Framework 3.5.1 (3122648) (Important) Microsoft .NET Framework 3.5.1 (3127220) (Important) Microsoft .NET Framework 4.5.2 (3122656) (Important) Microsoft .NET Framework 4.5.2 (3127229) (Important)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3133043) (Important)	Not applicable
Windows Server 2012	Windows Server 2012 (Server	Windows Server 2012 (Server Core	Microsoft .NET Framework 3.5	Not applicable	Windows Server 2012	Not applicable

(Server Core installation)	Core installation) (3126446) (Important)	installation) (3134214) (Important)	(3122649) (Important) Microsoft .NET Framework 3.5 (3127221) (Important) Microsoft .NET Framework 4.5.2 (3122655) (Important) Microsoft .NET Framework 4.5.2 (3127227) (Important) Microsoft .NET Framework 4.6/4.6.1 (3122658) (Important) Microsoft .NET Framework 4.6/4.6.1 (3127230) (Important)		(Server Core installation) (3133043) (Important)	
Windows Server 2012 R2 (Server Core installation)	Windows Server 2012 R2 (Server Core installation) (3126446) (Important)	Windows Server 2012 R2 (Server Core installation) (3134214) (Important)	Microsoft .NET Framework 3.5 (3122651) (Important) Microsoft .NET Framework 3.5 (3127222) (Important) Microsoft .NET Framework 4.5.2 (3122654) (Important) Microsoft .NET Framework 4.5.2 (3127226) (Important) Microsoft .NET Framework 4.6/4.6.1 (3122660) (Important) Microsoft .NET Framework 4.6/4.6.1 (3127231) (Important)	Active Directory Federation Services 3.0 (3134222) (Important)	Windows Server 2012 R2 (Server Core installation) (3133043) (Important)	Not applicable

Microsoft Office Suites and Software

Microsoft Office 2007	
Bulletin Identifier	**MS16-015**
Aggregate Severity Rating	**Critical**
Microsoft Office 2007 Service Pack 3	Microsoft Office 2007 Service Pack 3 (3114742) (Important) Microsoft Excel 2007 Service Pack 3 (3114741) (Important) Microsoft Word 2007 Service Pack 3 (3114748) (Critical)
Microsoft Office 2010	
Bulletin Identifier	**MS16-015**
Aggregate Severity Rating	**Critical**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3114752) (Important) Microsoft Excel 2010 Service Pack 2 (32-bit editions) (3114759) (Important) Microsoft Word 2010 Service Pack 2 (32-bit editions) (3114755) (Critical)
Microsoft Office 2010 Service Pack 2 (64-bit editions)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3114752) (Important) Microsoft Excel 2010 Service Pack 2 (64-bit editions) (3114759) (Important) Microsoft Word 2010 Service Pack 2 (64-bit editions) (3114755) (Critical)
Microsoft Office 2013	
Bulletin Identifier	**MS16-015**
Aggregate Severity Rating	**Critical**
Microsoft Office 2013 Service Pack 1 (32-bit editions)	Microsoft Excel 2013 Service Pack 1 (32-bit editions) (3114734) (Important) Microsoft Word 2013 Service Pack 1 (32-bit editions) (3114724) (Critical)
Microsoft Office 2013 Service Pack 1 (64-bit editions)	Microsoft Excel 2013 Service Pack 1 (64-bit editions)

	(3114734) (Important) Microsoft Word 2013 Service Pack 1 (64-bit editions) (3114724) (Critical)
Microsoft Office 2013 RT	
Bulletin Identifier	**MS16-015**
Aggregate Severity Rating	**Critical**
Microsoft Office 2013 RT Service Pack 1	Microsoft Excel 2013 RT Service Pack 1 (3114734) (Important) Microsoft Word 2013 RT Service Pack 1 (3114724) (Critical)
Microsoft Office 2016	
Bulletin Identifier	**MS16-015**
Aggregate Severity Rating	**Critical**
Microsoft Office 2016 (32-bit edition)	Microsoft Excel 2016 (32-bit edition) (3114698) (Important) Microsoft Word 2016 (32-bit edition) (3114702) (Critical)
Microsoft Office 2016 (64-bit edition)	Microsoft Excel 2016 (64-bit edition) (3114698) (Important) Microsoft Word 2016 (64-bit edition) (3114702) (Critical)
Microsoft Office for Mac	
Bulletin Identifier	**MS16-015**
Aggregate Severity Rating	**Critical**
Microsoft Office for Mac 2011	Microsoft Excel for Mac 2011 (3137721) (Important) Microsoft Word for Mac 2011 (3137721) (Critical)
Microsoft Office 2016 for Mac	Microsoft Excel 2016 for Mac (3134241) (Important) Microsoft Word 2016 for Mac (3134241) (Critical)
Other Office Software	

Bulletin Identifier	**MS16-015**
Aggregate Severity Rating	**Important**
Microsoft Office Compatibility Pack Service Pack 3	Microsoft Office Compatibility Pack Service Pack 3 (3114548) (Important) Microsoft Office Compatibility Pack Service Pack 3 (3114745) (Important)
Microsoft Excel Viewer	Microsoft Excel Viewer (3114747) (Important)
Microsoft Word Viewer	Microsoft Word Viewer (3114773) (Important)

Note for MS16-015

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

Microsoft Office Services and Web Apps

Microsoft SharePoint Server 2007	
Bulletin Identifier	**MS16-015**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2007 Service Pack 3 (32-bit editions)	Excel Services (3114432) (Important)
Microsoft SharePoint Server 2007 Service Pack 3 (64-bit editions)	Excel Services (3114432) (Important)
Microsoft SharePoint Server 2010	
Bulletin Identifier	**MS16-015**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2010 Service Pack 2	Excel Services (3114401) (Important)
Microsoft SharePoint Server 2013	
Bulletin Identifier	**MS16-015**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2013 Service Pack 1	Excel Services (3114335) (Important) Word Automation Services

	(3114481) (Important)
Microsoft Office Web Apps 2010	
Bulletin Identifier	**MS16-015**
Aggregate Severity Rating	**Important**
Microsoft Office Web Apps 2010 Service Pack 2	Microsoft Office Web Apps 2010 Service Pack 2 (3114407) (Important)
Microsoft Office Web Apps 2013	
Bulletin Identifier	**MS16-015**
Aggregate Severity Rating	**Important**
Microsoft Office Web Apps 2013 Service Pack 1	Microsoft Office Web Apps Server 2013 Service Pack 1 (3114338) (Important)

Note for MS16-015

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

Microsoft Server Software

Microsoft SharePoint Server 2013	
Bulletin Identifier	**MS16-015**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2013 Service Pack 1	Microsoft SharePoint Server 2013 Service Pack 1 (3039768) (Important)
Microsoft SharePoint Foundation 2013	
Bulletin Identifier	**MS16-015**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Foundation 2013 Service Pack 1	Microsoft SharePoint Foundation 2013 Service Pack 1 (3114733) (Important)

Note for MS16-015

This bulletin spans more than one software category. See the 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

Revisions

- V1.0 (February 9, 2016): Bulletin Summary published.
- V2.0 (February 10, 2016): For MS16-014, Bulletin Summary revised to announce the availability of update 3126041 for Microsoft Windows Vista, Windows Server 2008, Windows Server 2008 for Itanium-based Systems, Windows 8.1, and Windows Server 2012 R2. Customers should apply the applicable updates to be protected from the vulnerabilities discussed in this bulletin. The majority of customers have automatic updating enabled and will not need to take any action because the updates will be downloaded and installed automatically. For MS16-021, corrected the Exploitability Assessment for CVE-2016-0050.
- V3.0 (February 16, 2016): For MS16-015, added the 3134241 update for Microsoft Office 2016 for Mac, and the 3137721 update for Microsoft Office for Mac 2011, which are available as of February 16, 2016. For more information, see Microsoft Knowledge Base Article 3134241 and Microsoft Knowledge Base Article 3137721.
- V3.1 (February 24, 2016): Added a Known Issues reference to the Executive Summaries table for MS16-014. For more information, see Microsoft Knowledge Base Article 3126041. Please also note that a second Known Issue, which includes workarounds, has been added to Microsoft Knowledge Base Article 3126587.

Page generated 2016-02-24 13:45-08:00.