Microsoft Security Bulletin Summary for January 2016

Published: January 12, 2016 | Updated: February 19, 2016

Version: 1.3

This bulletin summary lists security bulletins released for January 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
MS16-001	**Cumulative Security Update for Internet Explorer (3124903)** This security update resolves vulnerabilities in Internet Explorer. The more 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	---------	Microsoft Windows, Internet Explorer
MS16-002	**Cumulative Security Update for Microsoft Edge (3124904)** This security update resolves vulnerabilities in Microsoft Edge. 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
MS16-003	**Cumulative Security Update for JScript and VBScript to Address Remote Code Execution (3125540)**	Critical Remote Code Execution	May require restart	---------	Microsoft Windows

	This security update resolves a vulnerability in the VBScript scripting engine in Microsoft Windows. The vulnerability could allow remote code execution if a user visits a specially crafted website. 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.				
MS16-004	**Security Update for Microsoft Office to Address Remote Code Execution (3124585)** 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	3114503 2920727 2881029 2881067 3039794 3124585	Microsoft Office, Visual Basic
MS16-005	**Security Update for Windows Kernel-Mode Drivers to Address Remote Code Execution (3124584)** This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if a user visits a malicious website.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows
MS16-006	**Security Update for Silverlight to Address Remote Code Execution (3126036)** This security update resolves a vulnerability in Microsoft Silverlight. The vulnerability could allow remote code execution if a user visits a compromised website that contains a specially crafted Silverlight application. An attacker would have no way to force users to visit a compromised website. Instead, an attacker would have to convince users to visit the website, typically by getting them to click a link in an email or instant message that takes users to the attacker's website.	Critical Remote Code Execution	Does not require a restart	---------	Microsoft Silverlight
MS16-007	**Security Update for Microsoft Windows to Address Remote Code Execution (3124901)** 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	3124266 3124263	Microsoft Windows

MS16-008	**Security Update for Windows Kernel to Address Elevation of Privilege (3124605)** 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.	Important Elevation of Privilege	Requires restart	---------	Microsoft Windows
MS16-010	**Security Update in Microsoft Exchange Server to Address Spoofing (3124557)** This security update resolves vulnerabilities in Microsoft Exchange Server. The most severe of the vulnerabilities could allow spoofing if Outlook Web Access (OWA) fails to properly handle web requests, and sanitize user input and email content.	Important Spoofing	May require restart	---------	Microsoft Exchange Server

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
MS16-001: Cumulative Security Update for Internet Explorer (3124903)				
CVE-2016-0002	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not Applicable
CVE-2016-0005	Internet Explorer Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not Applicable
MS16-002: Cumulative Security Update for Microsoft Edge (3124904)				
CVE-2016-0003	Microsoft Edge Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not Applicable
CVE-2016-0024	Scripting Engine Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not Applicable
MS16-003: Cumulative Security Update for JScript and VBScript to Address Remote Code Execution (3125540)				

CVE-2016-0002	Scripting Engine Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not Applicable
MS16-004: Security Update for Microsoft Office to Address Remote Code Execution (3124585)				
CVE-2015-6117	Microsoft SharePoint Security Feature Bypass Vulnerability	4 - Not affected	3- Exploitation Unlikely	Not Applicable
CVE-2016-0010	Microsoft Office Memory Corruption Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not Applicable
CVE-2016-0011	Microsoft SharePoint Security Feature Bypass Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not Applicable
CVE-2016-0012	Microsoft Office ASLR Bypass	1- Exploitation More Likely	1- Exploitation More Likely	Not Applicable
CVE-2016-0035	Microsoft Office Memory Corruption Vulnerability	1- Exploitation More Likely	1- Exploitation More Likely	Not Applicable
MS16-005: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3124584)				
CVE-2016-0008	Windows GDI32.dll ASLR Bypass Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not Applicable
CVE-2016-0009	Win32k Remote Code Execution Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not Applicable
MS16-006: Security Update for Silverlight to Address Remote Code Execution (3126036)				
CVE-2016-0034	Silverlight Runtime Remote Code Execution Vulnerability	0 - Exploitation Detected	0 - Exploitation Detected	Not Applicable
MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution (3124901)				
CVE-2016-0014	DLL Loading Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not Applicable
CVE-2016-0015	DirectShow Heap Corruption Remote Code Execution Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not Applicable
CVE-2016-0016	DLL Loading Remote Code	1 - Exploitation More Likely	1 - Exploitation More Likely	Not Applicable

	Execution Vulnerability			
CVE-2016-0018	DLL Loading Remote Code Execution Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not Applicable
CVE-2016-0019	Windows Remote Desktop Protocol Security Bypass Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not Applicable
CVE-2016-0020	MAPI DLL Loading Elevation of Privilege Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not Applicable
MS16-008: Security Update for Windows Kernel to Address Elevation of Privilege (3124605)				
CVE-2016-0006	Windows Mount Point Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not Applicable
CVE-2016-0007	Windows Mount Point Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not Applicable
MS16-010: Security Update in Microsoft Exchange Server to Address Spoofing (3124557)				
CVE-2016-0029	Exchange Spoofing Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not Applicable
CVE-2016-0030	Exchange Spoofing Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not Applicable
CVE-2016-0031	Exchange Spoofing Vulnerability	2 - Exploitation Less Likely	4 - Not affected	Not Applicable
CVE-2016-0032	Exchange Spoofing Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	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	**MS16-001**	**MS16-002**	**MS16-003**	**MS16-005**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**
Windows Vista Service Pack 2	Internet Explorer 8 (3124275) (Critical) Internet Explorer 9 (3124275) (Critical)	Not applicable	VBScript 5.7 (3124624) (Critical)	Windows Vista Service Pack 2 (3124000) (Critical) Windows Vista Service Pack 2 (3124001) (Important)
Windows Vista x64 Edition Service Pack 2	Internet Explorer 8 (3124275) (Critical) Internet Explorer 9 (3124275) (Critical)	Not applicable	VBScript 5.7 (3124624) (Critical)	Windows Vista x64 Edition Service Pack 2 (3124000) (Critical) Windows Vista x64 Edition Service Pack 2 (3124001) (Important)
Windows Server 2008				
Bulletin Identifier	**MS16-001**	**MS16-002**	**MS16-003**	**MS16-005**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**Critical**
Windows Server 2008 for 32-bit Systems Service Pack 2	Internet Explorer 8 (3124275) (Moderate) Internet Explorer 9 (3124275) (Moderate)	Not applicable	VBScript 5.7 (3124624) (Critical)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3124000) (Critical) Windows Server 2008 for 32-bit Systems Service Pack 2 (3124001) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Internet Explorer 8 (3124275) (Moderate) Internet Explorer 9 (3124275) (Moderate)	Not applicable	VBScript 5.7 (3124624) (Critical)	Windows Server 2008 for x64-based Systems Service Pack 2 (3124000) (Critical) Windows Server 2008 for x64-based Systems Service Pack 2 (3124001) (Important)
Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Not applicable	VBScript 5.7 (3124624) (Critical)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3124000) (Critical) Windows Server 2008 for Itanium-based Systems Service Pack 2 (3124001) (Important)
Windows 7				

Bulletin Identifier	**MS16-001**	**MS16-002**	**MS16-003**	**MS16-005**
Aggregate Severity Rating	**Critical**	**None**	**None**	**Critical**
Windows 7 for 32-bit Systems Service Pack 1	Internet Explorer 8 (3124275) (Critical) Internet Explorer 9 (3124275) (Critical) Internet Explorer 10 (3124275) (Critical) Internet Explorer 11 (3124275) (Critical)	Not applicable	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3124000) (Critical) Windows 7 for 32-bit Systems Service Pack 1 (3124001) (Important)
Windows 7 for x64-based Systems Service Pack 1	Internet Explorer 8 (3124275) (Critical) Internet Explorer 9 (3124275) (Critical) Internet Explorer 10 (3124275) (Critical) Internet Explorer 11 (3124275) (Critical)	Not applicable	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3124000) (Critical) Windows 7 for x64-based Systems Service Pack 1 (3124001) (Important)
Windows Server 2008 R2				
Bulletin Identifier	**MS16-001**	**MS16-002**	**MS16-003**	**MS16-005**
Aggregate Severity Rating	**Moderate**	**None**	**None**	**Critical**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Internet Explorer 8 (3124275) (Moderate) Internet Explorer 9 (3124275) (Moderate) Internet Explorer 10 (3124275) (Moderate)	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3124000) (Critical) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3124001) (Important)

	Internet Explorer 11 (3124275) (Moderate)			
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Internet Explorer 8 (3124275) (Moderate)	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3124000) (Critical) Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3124001) (Important)
Windows 8 and Windows 8.1				
Bulletin Identifier	**MS16-001**	**MS16-002**	**MS16-003**	**MS16-005**
Aggregate Severity Rating	**Critical**	**None**	**None**	**Important**
Windows 8 for 32-bit Systems	Internet Explorer 10 (3124275) (Critical)	Not applicable	Not applicable	Windows 8 for 32-bit Systems (3124001) (Important)
Windows 8 for x64-based Systems	Internet Explorer 10 (3124275) (Critical)	Not applicable	Not applicable	Windows 8 for x64-based Systems (3124001) (Important)
Windows 8.1 for 32-bit Systems	Internet Explorer 11 (3124275) (Critical)	Not applicable	Not applicable	Windows 8.1 for 32-bit Systems (3124001) (Important)
Windows 8.1 for x64-based Systems	Internet Explorer 11 (3124275) (Critical)	Not applicable	Not applicable	Windows 8.1 for x64-based Systems (3124001) (Important)
Windows Server 2012 and Windows Server 2012 R2				
Bulletin Identifier	**MS16-001**	**MS16-002**	**MS16-003**	**MS16-005**
Aggregate Severity Rating	**Moderate**	**None**	**None**	**Important**
Windows Server 2012	Internet Explorer 10 (3124275) (Moderate)	Not applicable	Not applicable	Windows Server 2012 (3124001) (Important)
Windows Server 2012 R2	Internet Explorer 11 (3124275) (Moderate)	Not applicable	Not applicable	Windows Server 2012 R2 (3124001) (Important)
Windows RT and Windows RT 8.1				
Bulletin	**MS16-001**	**MS16-002**	**MS16-003**	**MS16-005**

Identifier				
Aggregate Severity Rating	**Critical**	**None**	**None**	**Important**
Windows RT	Internet Explorer 10 (3124275) (Critical)	Not applicable	Not applicable	Windows RT (3124001) (Important)
Windows RT 8.1	Internet Explorer 11 (3124275) (Critical)	Not applicable	Not applicable	Windows RT 8.1 (3124001) (Important)
Windows 10				
Bulletin Identifier	**MS16-001**	**MS16-002**	**MS16-003**	**MS16-005**
Aggregate Severity Rating	**Critical**	**Critical**	**None**	**Important**
Windows 10 for 32-bit Systems	Internet Explorer 11 (3124266) (Critical)	Microsoft Edge (3124266) (Critical)	Not applicable	Windows 10 for 32-bit Systems (3124266) (Important)
Windows 10 for x64-based Systems	Internet Explorer 11 (3124266) (Critical)	Microsoft Edge (3124266) (Critical)	Not applicable	Windows 10 for x64-based Systems (3124266) (Important)
Windows 10 Version 1511 for 32-bit Systems	Internet Explorer 11 (3124263) (Critical)	Microsoft Edge (3124263) (Critical)	Not applicable	Windows 10 Version 1511 for 32-bit Systems (3124263) (Important)
Windows 10 Version 1511 for x64-based Systems	Internet Explorer 11 (3124263) (Critical)	Microsoft Edge (3124263) (Critical)	Not applicable	Windows 10 Version 1511 for x64-based Systems (3124263) (Important)
Server Core installation option				
Bulletin Identifier	**MS16-001**	**MS16-002**	**MS16-003**	**MS16-005**
Aggregate Severity Rating	**None**	**None**	**Critical**	**Critical**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	VBScript 5.7 (3124624) (Critical)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3124000) (Critical) Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3124001) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	VBScript 5.7 (3124624) (Critical)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3124000) (Critical)

				Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3124001) (Important)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Not applicable	Not applicable	VBScript 5.8 (3124625) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3124000) (Critical) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3124001) (Important)
Windows Server 2012 (Server Core installation)	Not applicable	Not applicable	Not applicable	Windows Server 2012 (Server Core installation) (3124001) (Important)
Windows Server 2012 R2 (Server Core installation)	Not applicable	Not applicable	Not applicable	Windows Server 2012 R2 (Server Core installation) (3124001) (Important)

Windows Operating Systems and Components (Table 2 of 2)

Windows Vista		
Bulletin Identifier	**MS16-007**	**MS16-008**
Aggregate Severity Rating	**Important**	**Important**
Windows Vista Service Pack 2	Windows Vista Service Pack 2 (3121918) (Important) Windows Vista Service Pack 2 (3109560) (Important) Windows Vista Service Pack 2 (3110329) (Important) Windows Vista Service Pack 2 (3108664) (Important)	Windows Vista Service Pack 2 (3121212) (Important)
Windows Vista x64 Edition Service Pack 2	Windows Vista x64 Edition Service Pack 2 (3121918) (Important) Windows Vista x64 Edition Service Pack 2 (3109560) (Important) Windows Vista x64 Edition Service Pack 2	Windows Vista x64 Edition Service Pack 2 (3121212) (Important)

	(3110329) (Important) Windows Vista x64 Edition Service Pack 2 (3108664) (Important)	
Windows Server 2008		
Bulletin Identifier	**MS16-007**	**MS16-008**
Aggregate Severity Rating	**Important**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2	Windows Server 2008 for 32-bit Systems Service Pack 2 (3121918) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (3109560) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (3110329) (Important) Windows Server 2008 for 32-bit Systems Service Pack 2 (3108664) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3121212) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Windows Server 2008 for x64-based Systems Service Pack 2 (3121918) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (3109560) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (3110329) (Important) Windows Server 2008 for x64-based Systems Service Pack 2 (3108664) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (3121212) (Important)
Windows Server 2008 for Itanium-based Systems Service Pack 2	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3121918) (Important) Windows Server 2008 for Itanium-based Systems Service Pack 2 (3109560) (Important) Windows Server 2008 for Itanium-based Systems Service Pack 2 (3110329)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3121212) (Important)

	(Important) Windows Server 2008 for Itanium-based Systems Service Pack 2 (3108664) (Important)	
Windows 7		
Bulletin Identifier	**MS16-007**	**MS16-008**
Aggregate Severity Rating	**Important**	**Important**
Windows 7 for 32-bit Systems Service Pack 1	Windows 7 for 32-bit Systems Service Pack 1 (3121918) (Important) Windows 7 for 32-bit Systems Service Pack 1 (3109560) (Important) Windows 7 for 32-bit Systems Service Pack 1 (3110329) (Important) Windows 7 for 32-bit Systems Service Pack 1 (3121461) (Important) Windows 7 for 32-bit Systems Service Pack 1 (3108664) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3121212) (Important)
Windows 7 for x64-based Systems Service Pack 1	Windows 7 for x64-based Systems Service Pack 1 (3121918) (Important) Windows 7 for x64-based Systems Service Pack 1 (3109560) (Important) Windows 7 for x64-based Systems Service Pack 1 (3110329) (Important) Windows 7 for x64-based Systems Service Pack 1 (3121461) (Important) Windows 7 for x64-based Systems Service Pack 1 (3108664) (Important)	Windows 7 for x64-based Systems Service Pack 1 (3121212) (Important)
Windows Server 2008 R2		
Bulletin Identifier	**MS16-007**	**MS16-008**
Aggregate Severity Rating	**Important**	**Important**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Windows Server 2008 R2 for x64-based Systems Service Pack 1	Windows Server 2008 R2 for x64-based Systems Service Pack 1

	(3121918) (Important) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3109560) (Important) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3110329) (Important) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3108664) (Important)	(3121212) (Important)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3121918) (Important) Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3109560) (Important) Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3110329) (Important) Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3108664) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3121212) (Important)
Windows 8 and Windows 8.1		
Bulletin Identifier	**MS16-007**	**MS16-008**
Aggregate Severity Rating	**Important**	**Important**
Windows 8 for 32-bit Systems	Windows 8 for 32-bit Systems (3121918) (Important) Windows 8 for 32-bit Systems (3109560) (Important) Windows 8 for 32-bit Systems (3110329) (Important) Windows 8 for 32-bit Systems (3121461) (Important)	Windows 8 for 32-bit Systems (3121212) (Important)
Windows 8 for x64-based Systems	Windows 8 for x64-based Systems (3121918) (Important) Windows 8 for x64-based Systems (3109560)	Windows 8 for x64-based Systems (3121212) (Important)

	(Important) Windows 8 for x64-based Systems (3110329) (Important) Windows 8 for x64-based Systems (3121461) (Important)	
Windows 8.1 for 32-bit Systems	Windows 8.1 for 32-bit Systems (3121918) (Important) Windows 8.1 for 32-bit Systems (3109560) (Important) Windows 8.1 for 32-bit Systems (3110329) (Important) Windows 8.1 for 32-bit Systems (3121461) (Important)	Windows 8.1 for 32-bit Systems (3121212) (Important)
Windows 8.1 for x64-based Systems	Windows 8.1 for x64-based Systems (3121918) (Important) Windows 8.1 for x64-based Systems (3109560) (Important) Windows 8.1 for x64-based Systems (3110329) (Important) Windows 8.1 for x64-based Systems (3121461) (Important)	Windows 8.1 for x64-based Systems (3121212) (Important)
Windows Server 2012 and Windows Server 2012 R2		
Bulletin Identifier	**MS16-007**	**MS16-008**
Aggregate Severity Rating	**Important**	**Important**
Windows Server 2012	Windows Server 2012 (3121918) (Important) Windows Server 2012 (3109560) (Important) Windows Server 2012 (3110329) (Important)	Windows Server 2012 (3121212) (Important)
Windows Server 2012 R2	Windows Server 2012 R2 (3121918) (Important) Windows Server 2012 R2 (3109560)	Windows Server 2012 R2 (3121212) (Important)

	(Important) Windows Server 2012 R2 (3110329) (Important) Windows Server 2012 R2 (3121461) (Important)	
Windows RT and Windows RT 8.1		
Bulletin Identifier	**MS16-007**	**MS16-008**
Aggregate Severity Rating	**Important**	**Important**
Windows RT	Windows RT (3121918) (Important) Windows RT (3110329) (Important)	Windows RT (3121212) (Important)
Windows RT 8.1	Windows RT 8.1 (3121918) (Important) Windows RT 8.1 (3110329) (Important)	Windows RT 8.1 (3121212) (Important)
Windows 10		
Bulletin Identifier	**MS16-007**	**MS16-008**
Aggregate Severity Rating	**Important**	**Important**
Windows 10 for 32-bit Systems	Windows 10 for 32-bit Systems (3124266) (Important)	Windows 10 for 32-bit Systems (3124266) (Important)
Windows 10 for x64-based Systems	Windows 10 for x64-based Systems (3124266) (Important)	Windows 10 for x64-based Systems (3124266) (Important)
Windows 10 Version 1511 for 32-bit Systems	Windows 10 Version 1511 for 32-bit Systems (3124263) (Important)	Windows 10 Version 1511 for 32-bit Systems (3124263) (Important)
Windows 10 Version 1511 for x64-based Systems	Windows 10 Version 1511 for x64-based Systems (3124263) (Important)	Windows 10 Version 1511 for x64-based Systems (3124263) (Important)
Server Core installation option		
Bulletin Identifier	**MS16-007**	**MS16-008**
Aggregate Severity Rating	**Important**	**Important**
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

(Server Core installation)	(Server Core installation) (3121918) (Important)	(Server Core installation) (3121212) (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) (3121918) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3121212) (Important)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3121918) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3121212) (Important)
Windows Server 2012 (Server Core installation)	Windows Server 2012 (Server Core installation) (3121918) (Important)	Windows Server 2012 (Server Core installation) (3121212) (Important)
Windows Server 2012 R2 (Server Core installation)	Windows Server 2012 R2 (Server Core installation) (3121918) (Important)	Windows Server 2012 R2 (Server Core installation) (3121212) (Important)

Microsoft Office Suites and Software

Microsoft Office 2007	
Bulletin Identifier	**MS16-004**
Aggregate Severity Rating	**Critical**
Microsoft Office 2007 Service Pack 3	Microsoft Office 2007 Service Pack 3 (2881067) (Important) Microsoft Office 2007 Service Pack 3 (3114541) (Critical) Microsoft Excel 2007 Service Pack 3 (3114540) (Important) Microsoft PowerPoint 2007 Service Pack 3 (3114429) (Important) Microsoft Visio 2007 Service Pack 3 (3114421) (Important) Microsoft Word 2007 Service Pack 3 (3114549) (Important)
Microsoft Office 2010	
Bulletin Identifier	**MS16-004**

Aggregate Severity Rating	**Critical**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (2881029) (Important) Microsoft Office 2010 Service Pack 2 (32-bit editions) (3114553) (Critical) Microsoft Office 2010 Service Pack 2 (32-bit editions) (3114554) (Important) Microsoft Excel 2010 Service Pack 2 (32-bit editions) (3114564) (Important) Microsoft PowerPoint 2010 Service Pack 2 (32-bit editions) (3114396) (Important) Microsoft Visio 2010 Service Pack 2 (32-bit editions) (3114402) (Important) Microsoft Word 2010 Service Pack 2 (32-bit editions) (3114557) (Important)
Microsoft Office 2010 Service Pack 2 (64-bit editions)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3114553) (Critical) Microsoft Office 2010 Service Pack 2 (64-bit editions) (3114554) (Important) Microsoft Office 2010 Service Pack 2 (64-bit editions) (3114564) (Important) Microsoft Excel 2010 Service Pack 2 (64-bit editions) (3114564) (Important) Microsoft PowerPoint 2010 Service Pack 2 (64-bit editions) (3114396) (Important) Microsoft Visio 2010 Service Pack 2 (64-bit editions) (3114402) (Important) Microsoft Word 2010 Service Pack 2 (64-bit editions) (3114557) (Important)
Microsoft Office 2013	
Bulletin Identifier	**MS16-004**
Aggregate Severity Rating	**Critical**
Microsoft Office 2013 Service Pack 1 (32-bit editions)	Microsoft Office 2013 Service Pack 1 (32-bit editions) (3039794)

	(Important) Microsoft Office 2013 Service Pack 1 (32-bit editions) (3114486) (Critical) Microsoft Excel 2013 Service Pack 1 (32-bit editions) (3114504) (Important) Microsoft PowerPoint 2013 Service Pack 1 (32-bit editions) (3114482) (Important) Microsoft Visio 2013 Service Pack 1 (32-bit editions) (3114489) (Important) Microsoft Word 2013 Service Pack 1 (32-bit editions) (3114494) (Important)
Microsoft Office 2013 Service Pack 1 (64-bit editions)	Microsoft Office 2013 Service Pack 1 (64-bit editions) (3114486) (Critical) Microsoft Excel 2013 Service Pack 1 (64-bit editions) (3114504) (Important) Microsoft PowerPoint 2013 Service Pack 1 (64-bit editions) (3114482) (Important) Microsoft Visio 2013 Service Pack 1 (64-bit editions) (3114489) (Important) Microsoft Word 2013 Service Pack 1 (64-bit editions) (3114494) (Important)
Microsoft Office 2013 RT	
Bulletin Identifier	**MS16-004**
Aggregate Severity Rating	**Critical**
Microsoft Office 2013 RT Service Pack 1	Microsoft Office 2013 RT Service Pack 1 (3114486) (Critical) Microsoft Excel 2013 RT Service Pack 1 (3114504) (Important) Microsoft PowerPoint 2013 RT Service Pack 1 (3114482) (Important) Microsoft Word 2013 RT Service Pack 1 (3114494) (Important)
Microsoft Office 2016	

Bulletin Identifier	**MS16-004**
Aggregate Severity Rating	**Critical**
Microsoft Office 2016 (32-bit edition)	Microsoft Office 2016 (32-bit edition) (2920727) (Important) Microsoft Office 2016 (32-bit edition) (3114527) (Critical) Microsoft Excel 2016 (32-bit edition) (3114520) (Important) Microsoft PowerPoint 2016 (32-bit edition) (3114518) (Important) Microsoft Visio 2016 (32-bit edition) (3114511) (Important) Microsoft Word 2016 (32-bit edition) (3114526) (Important)
Microsoft Office 2016 (64-bit edition)	Microsoft Office 2016 (64-bit edition) (3114527) (Critical) Microsoft Office 2016 (64-bit edition) (3114520) (Important) Microsoft Excel 2016 (64-bit edition) (3114520) (Important) Microsoft PowerPoint 2016 (64-bit edition) (3114518) (Important) Microsoft Visio 2016 (64-bit edition) (3114511) (Important) Microsoft Word 2016 (64-bit edition) (3114526) (Important)
Microsoft Office for Mac	
Bulletin Identifier	**MS16-004**
Aggregate Severity Rating	**Critical**
Microsoft Office for Mac 2011	Microsoft Excel for Mac 2011 (3133699) (Critical) Microsoft PowerPoint for Mac 2011 (3133699) (Critical)

	Microsoft Word for Mac 2011 (3133699) (Critical)
Microsoft Office 2016 for Mac	Microsoft Excel 2016 for Mac (3133711) (Critical) Microsoft PowerPoint 2016 for Mac (3133711) (Critical) Microsoft Word 2016 for Mac (3133711) (Critical)
Other Office Software	
Bulletin Identifier	**MS16-004**
Aggregate Severity Rating	**Critical**
Microsoft Office Compatibility Pack Service Pack 3	Microsoft Office Compatibility Pack Service Pack 3 (3114546) (Important)
Microsoft Excel Viewer	Microsoft Excel Viewer (3114547) (Important)
Microsoft Word Viewer	Microsoft Word Viewer (3114569) (Critical)

Note for MS16-004

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

Microsoft Developer Tools and Software

Microsoft Silverlight	
Bulletin Identifier	**MS16-006**
Aggregate Severity Rating	**Critical**
Microsoft Silverlight 5	Microsoft Silverlight 5 when installed on Mac (3126036) (Critical) Microsoft Silverlight 5 Developer Runtime when installed on Mac (3126036) (Critical) Microsoft Silverlight 5 when installed on all supported releases of Microsoft Windows clients (3126036) (Critical) Microsoft Silverlight 5 Developer Runtime when installed on all supported releases of Microsoft Windows clients

	(3126036) (Critical) Microsoft Silverlight 5 when installed on all supported releases of Microsoft Windows servers (3126036) (Critical) Microsoft Silverlight 5 Developer Runtime when installed on all supported releases of Microsoft Windows servers (3126036) (Critical)

Microsoft Server Software

Microsoft SharePoint Server 2013		
Bulletin Identifier	**MS16-004**	**MS16-010**
Aggregate Severity Rating	**Important**	**None**
Microsoft SharePoint Server 2013 Service Pack 1	Microsoft SharePoint Server 2013 Service Pack 1 (3114503) (Important)	Not applicable
Microsoft SharePoint Foundation 2013		
Bulletin Identifier	**MS16-004**	**MS16-010**
Aggregate Severity Rating	**Important**	**None**
Microsoft SharePoint Foundation 2013 Service Pack 1	Microsoft SharePoint Foundation 2013 Service Pack 1 (3114503) (Important)	Not applicable
Microsoft Exchange Server 2013		
Bulletin Identifier	**MS16-004**	**MS16-010**
Aggregate Severity Rating	**None**	**Important**
Microsoft Exchange Server 2013 Service Pack 1	Not applicable	Microsoft Exchange Server 2013 Service Pack 1 (3124557) (Important)
Microsoft Exchange Server 2013	Not applicable	Microsoft Exchange Server 2013 Cumulative Update 10 (3124557) (Important)
Microsoft Exchange Server 2013	Not applicable	Microsoft Exchange Server 2013 Cumulative Update 11 (3124557) (Important)
Microsoft Exchange Server 2016		
Bulletin Identifier	**MS16-004**	**MS16-010**

Aggregate Severity Rating	**None**	**Important**
Microsoft Exchange Server 2016	Not applicable	Microsoft Exchange Server 2016 (3124557) (Important)

Note for MS16-004

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

Microsoft Visual Basic Software

Microsoft Visual Basic Runtime 6.0	
Bulletin Identifier	**MS16-004**
Aggregate Severity Rating	**Important**
Visual Basic 6.0 Runtime	Visual Basic 6.0 Runtime (3096896) (Important)

Note for MS16-004

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 (January 12, 2016): Bulletin Summary published.
- V1.1 (January 13, 2016): Corrected the Exploitability Assessment for CVE-2016-0034. This is an informational change only.
- V1.2 (January 19, 2016): Added a Known Issues reference to the Executive Summaries table for MS16-004. See Microsoft Knowledge Base Article 3114503 for more information.
- V1.3 (February 19, 2016): For MS16-001, removed update 3124275 for Internet Explorer 7 from the Affected Software table because it is not affected by the vulnerabilities described in the bulletin. See Microsoft Knowledge Base Article 3124275 for more information. For MS16-004, added Known Issues references to the Executive Summaries table. For more information, see the following:
  - Microsoft Knowledge Base Article 2920727
  - Microsoft Knowledge Base Article 2881029
  - Microsoft Knowledge Base Article 2881067
  - Microsoft Knowledge Base Article 3039794
  - Microsoft Knowledge Base Article 3124585

Page generated 2016-02-22 10:14-08:00.