Microsoft Security Bulletin Summary for April 2016

Published: April 12, 2016 | Updated: September 12, 2017

Version: 4.0

This bulletin summary lists security bulletins released for April 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
MS16-037	**Cumulative Security Update for Internet Explorer (3148531)** 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 the vulnerabilities could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows, Internet Explorer
MS16-038	**Cumulative Security Update for Microsoft Edge (3148532)** 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 users with administrative user rights.	Critical Remote Code Execution	Requires restart	---------	Microsoft Windows, Microsoft Edge
MS16-039	**Security Update for Microsoft Graphics Component (3148522)** This security update resolves vulnerabilities in Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Skype for Business, and Microsoft Lync. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted	Critical Remote Code Execution	Requires restart	3148522	Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Skype for Business, Microsoft Lync.

	document or visits a webpage that contains specially crafted embedded fonts.				
MS16-040	**Security Update for Microsoft XML Core Services (3148541)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user clicks a specially crafted link that could allow an attacker to run malicious code remotely to take control of the user's system. However, in all cases an attacker would have no way to force a user to click a specially crafted link. An attacker would have to convince a user to click the link, typically by way of an enticement in an email or Instant Messenger message.	Critical Remote Code Execution	May require restart	---------	Microsoft Windows
MS16-041	**Security Update for .NET Framework (3148789)** This security update resolves a vulnerability in Microsoft .NET Framework. The vulnerability could allow remote code execution if an attacker with access to the local system executes a malicious application.	Important Remote Code Execution	May require restart	---------	Microsoft Windows, Microsoft .NET Framework
MS16-042	**Security Update for Microsoft Office (3148775)** 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	3148775	Microsoft Office, Microsoft Office Services and Web Apps
MS16-044	**Security Update for Windows OLE (3146706)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if Windows OLE fails to properly validate user input. An attacker could exploit the vulnerability to execute malicious code. However, an attacker must first convince a user to open either a specially crafted file or a program from either a webpage or an email message.	Important Remote Code Execution	Requires restart	3146706	Microsoft Windows
MS16-045	**Security Update for Windows Hyper-V (3143118)** This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an authenticated attacker on a guest operating system runs a specially crafted application that causes the Hyper-V host operating system to execute arbitrary code. Customers who have not enabled the Hyper-V role are not affected.	Important Remote Code Execution	Requires restart	---------	Microsoft Windows
MS16-046	**Security Update for Secondary Logon (3148538)** This security update resolves a vulnerability in Microsoft Windows. An attacker who successfully exploited this vulnerability could run arbitrary code as an administrator.	Important Elevation of Privilege	Requires restart	---------	Microsoft Windows

MS16-047	**Security Update for SAM and LSAD Remote Protocols (3148527)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker launches a man-in-the-middle (MiTM) attack. An attacker could then force a downgrade of the authentication level of the SAM and LSAD channels and impersonate an authenticated user.	Important Elevation of Privilege	Requires restart	---------	Microsoft Windows
MS16-048	**Security Update for CSRSS (3148528)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow security feature bypass if an attacker logs on to a target system and runs a specially crafted application.	Important Security Feature Bypass	Requires restart	3146723	Microsoft Windows
MS16-049	**Security Update for HTTP.sys (3148795)** This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow denial of service if an attacker sends a specially crafted HTTP packet to a target system.	Important Denial of Service	Requires restart	---------	Microsoft Windows
MS16-050	**Security Update for Adobe Flash Player (3154132)** This security update resolves vulnerabilities in Adobe Flash Player when installed on all supported editions of Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, 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
MS16-037: Cumulative Security Update for Internet Explorer (3148531)				
CVE-2016-0154	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0159	Internet Explorer Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2016-0160	DLL Loading Remote Code Execution	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable

	Vulnerability			
CVE-2016-0162	Internet Explorer Information Disclosure Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0164	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0166	Internet Explorer Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
MS16-038: Cumulative Security Update for Microsoft Edge (3148532)				
CVE-2016-0154	Microsoft Browser Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-0155	Microsoft Edge Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-0156	Microsoft Edge Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-0157	Microsoft Edge Memory Corruption Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-0158	Microsoft Edge Elevation of Privilege Vulnerability	1 - Exploitation More Likely	4 - Not affected	Not applicable
CVE-2016-0161	Microsoft Edge Elevation of Privilege Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Not applicable
MS16-039: Security Update for Microsoft Graphics Component (3148522)				
CVE-2016-0143	Win32k Elevation of Privilege Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Permanent
CVE-2016-0145	Graphics Memory Corruption Vulnerability	2 - Exploitation Less Likely	1 - Exploitation More Likely	Permanent
CVE-2016-0165	Win32k Elevation of Privilege Vulnerability	0 - Exploitation Detected	0 - Exploitation Detected	Permanent
CVE-2016-0167	Win32k Elevation of Privilege Vulnerability	0 - Exploitation Detected	0 - Exploitation Detected	Permanent
MS16-040: Security Update for Microsoft XML Core Services (3148541)				
CVE-2016-0147	MSXML 3.0 Remote Code Execution Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-041: Security Update for .NET Framework (3148789)				
CVE-2016-0148	.NET Framework Remote Code Execution Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable

MS16-042: Security Update for Microsoft Office (3148775)				
CVE-2016-0122	Microsoft Office Memory Corruption Vulnerability	1 - Exploitation More Likely	1 - Exploitation More Likely	Not applicable
CVE-2016-0127	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	2 - Exploitation Less Likely	Not applicable
CVE-2016-0136	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
CVE-2016-0139	Microsoft Office Memory Corruption Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
MS16-044: Security Update for Windows OLE (3146706)				
CVE-2016-0153	Windows OLE Remote Code Execution Vulnerability	4 - Not affected	1 - Exploitation More Likely	Not applicable
MS16-045: Security Update for Windows Hyper-V (3143118)				
CVE-2016-0088	Hyper-V Remote Code Execution Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Permanent
CVE-2016-0089	Hyper-V Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Permanent
CVE-2016-0090	Hyper-V Information Disclosure Vulnerability	4 - Not affected	3 - Exploitation Unlikely	Permanent
MS16-046: Security Update for Secondary Logon (3148538)				
CVE-2016-0135	Secondary Logon Elevation of Privilege Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Permanent
MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527)				
CVE-2016-0128	Windows SAM and LSAD Downgrade Vulnerability	3 - Exploitation Unlikely	3 - Exploitation Unlikely	Not applicable
MS16-048: Security Update for CSRSS (3148528)				
CVE-2016-0151	Windows CSRSS Security Feature Bypass Vulnerability	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not applicable
MS16-049: Security Update for HTTP.sys (3148795)				
CVE-2016-0150	HTTP.sys Denial of Service Vulnerability	3 - Exploitation Unlikely	4 - Not affected	Permanent
MS16-050: Security Update for Adobe Flash Player 3154132				
APSB16-10	See Adobe Security Bulletin APSB16-10 for	Not applicable	Not applicable	Not applicable

	vulnerability severity and update priority ratings.			

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	**MS16-037**	**MS16-038**	**MS16-039**	**MS16-040**	**MS16-041**	**MS16-044**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**Important**	**Important**
Windows Vista Service Pack 2	Internet Explorer 9 (4014661) (Critical)	Not applicable	Windows Vista Service Pack 2 (3145739) (Critical) Microsoft .NET Framework 3.0 Service Pack 2 (3142041) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Microsoft .NET Framework 4.6 (3143693) (Important)	Windows Vista Service Pack 2 (3146706) (Important)
Windows Vista x64 Edition Service Pack 2	Internet Explorer 9 (4014661) (Critical)	Not applicable	Windows Vista x64 Edition Service Pack 2 (3145739) (Critical) Microsoft .NET Framework 3.0 Service Pack 2 (3142041) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Microsoft .NET Framework 4.6 (3143693) (Important)	Windows Vista x64 Edition Service Pack 2 (3146706) (Important)
Windows Server 2008						
Bulletin Identifier	**MS16-037**	**MS16-038**	**MS16-039**	**MS16-040**	**MS16-041**	**MS16-044**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**Critical**	**Important**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2	Internet Explorer 9 (4014661) (Moderate)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3145739) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Microsoft .NET Framework 4.6 (3143693) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3146706) (Important)

			Microsoft .NET Framework 3.0 Service Pack 2 (3142041) (Critical)			
Windows Server 2008 for x64-based Systems Service Pack 2	Internet Explorer 9 (4014661) (Moderate)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3145739) (Critical) Microsoft .NET Framework 3.0 Service Pack 2 (3142041) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Microsoft .NET Framework 4.6 (3143693) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (3146706) (Important)
Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3145739) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3146706) (Important)
Windows 7						
Bulletin Identifier	**MS16-037**	**MS16-038**	**MS16-039**	**MS16-040**	**MS16-041**	**MS16-044**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**Important**	**Important**
Windows 7 for 32-bit Systems Service Pack 1	Internet Explorer 11 (4014661) (Critical)	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3145739) (Critical) Microsoft .NET Framework 3.5.1 (3142042) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Microsoft .NET Framework 4.6/4.6.1 (3143693) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3146706) (Important)
Windows 7 for x64-based Systems Service Pack 1	Internet Explorer 11 (4014661) (Critical)	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3145739) (Critical) Microsoft .NET Framework 3.5.1 (3142042) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Microsoft .NET Framework 4.6/4.6.1 (3143693) (Important)	Windows 7 for x64-based Systems Service Pack 1 (3146706) (Important)
Windows Server 2008 R2						
Bulletin Identifier	**MS16-037**	**MS16-038**	**MS16-039**	**MS16-040**	**MS16-041**	**MS16-044**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**Critical**	**Important**	**Important**

Windows Server 2008 R2 for x64-based Systems Service Pack 1	Internet Explorer 11 (4014661) (Moderate)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3145739) (Critical) Microsoft .NET Framework 3.5.1 (3142042) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Microsoft .NET Framework 4.6/4.6.1 (3143693) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3146706) (Important)
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3145739) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3146706) (Important)
Windows 8.1						
Bulletin Identifier	**MS16-037**	**MS16-038**	**MS16-039**	**MS16-040**	**MS16-041**	**MS16-044**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**None**	**Important**
Windows 8.1 for 32-bit Systems	Internet Explorer 11 (4014661) (Critical)	Not applicable	Windows 8.1 for 32-bit Systems (3145739) (Critical) Microsoft .NET Framework 3.5 (3142045) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Not applicable	Windows 8.1 for 32-bit Systems (3146706) (Important)
Windows 8.1 for x64-based Systems	Internet Explorer 11 (4014661) (Critical)	Not applicable	Windows 8.1 for x64-based Systems (3145739) (Critical) Microsoft .NET Framework 3.5 (3142045) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Not applicable	Windows 8.1 for x64-based Systems (3146706) (Important)
Windows Server 2012 and Windows Server 2012 R2						
Bulletin Identifier	**MS16-037**	**MS16-038**	**MS16-039**	**MS16-040**	**MS16-041**	**MS16-044**
Aggregate Severity Rating	**Moderate**	**None**	**Critical**	**Critical**	**None**	**Important**
Windows Server 2012	Internet Explorer 10 (4014661) (Moderate)	Not applicable	Windows Server 2012 (3145739) (Critical) Microsoft .NET Framework 3.5	Microsoft XML Core Services 3.0 (3146963) (Critical)	Not applicable	Windows Server 2012 (3146706) (Important)

			(3142043) (Critical)			
Windows Server 2012 R2	Internet Explorer 11 (4014661) (Moderate)	Not applicable	Windows Server 2012 R2 (3145739) (Critical) Microsoft .NET Framework 3.5 (3142045) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Not applicable	Windows Server 2012 R2 (3146706) (Important)
Windows RT 8.1						
Bulletin Identifier	**MS16-037**	**MS16-038**	**MS16-039**	**MS16-040**	**MS16-041**	**MS16-044**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Critical**	**None**	**Important**
Windows RT 8.1	Internet Explorer 11 (4014661) (Critical)	Not applicable	Windows RT 8.1 (3145739) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Not applicable	Windows RT 8.1 (3146706) (Important)
Windows 10						
Bulletin Identifier	**MS16-037**	**MS16-038**	**MS16-039**	**MS16-040**	**MS16-041**	**MS16-044**
Aggregate Severity Rating	**Critical**	**Critical**	**Critical**	**Critical**	**None**	**None**
Windows 10 for 32-bit Systems	Internet Explorer 11 (3147461) (Critical)	Microsoft Edge (3147461) (Critical)	Windows 10 for 32-bit Systems (3147461) (Critical) Microsoft .NET Framework 3.5 (3147461) (Critical)	Microsoft XML Core Services 3.0 (3147461) (Critical)	Not applicable	Not applicable
Windows 10 for x64-based Systems	Internet Explorer 11 (3147461) (Critical)	Microsoft Edge (3147461) (Critical)	Windows 10 for x64-based Systems (3147461) (Critical) Microsoft .NET Framework 3.5 (3147461) (Critical)	Microsoft XML Core Services 3.0 (3147461) (Critical)	Not applicable	Not applicable
Windows 10 Version 1511 for 32-bit Systems	Internet Explorer 11 (3147458) (Critical)	Microsoft Edge (3147458) (Critical)	Windows 10 Version 1511 for 32-bit Systems (3147458) (Critical) Microsoft .NET Framework 3.5 (3147458) (Critical)	Microsoft XML Core Services 3.0 (3147458) (Critical)	Not applicable	Not applicable

Windows 10 Version 1511 for x64-based Systems	Internet Explorer 11 (3147458) (Critical)	Microsoft Edge (3147458) (Critical)	Windows 10 Version 1511 for x64-based Systems (3147458) (Critical) Microsoft .NET Framework 3.5 (3147458) (Critical)	Microsoft XML Core Services 3.0 (3147458) (Critical)	Not applicable	Not applicable
Not applicable	Not applicable	Not applicable	Windows 10 Version 1703 for 32-bit Systems (4038788) (Critical)	Not applicable	Not applicable	Not applicable
Not applicable	Not applicable	Not applicable	Windows 10 Version 1703 for x64-based Systems (4038788) (Critical)	Not applicable	Not applicable	Not applicable
Server Core installation option						
Bulletin Identifier	**MS16-037**	**MS16-038**	**MS16-039**	**MS16-040**	**MS16-041**	**MS16-044**
Aggregate Severity Rating	**None**	**None**	**Critical**	**Critical**	**Important**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3145739) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3146706) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3145739) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3146706) (Important)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3145739) (Critical) Microsoft .NET Framework 3.5.1	Microsoft XML Core Services 3.0 (3146963) (Critical)	Microsoft .NET Framework 4.6/4.6.1 (3143693) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3146706) (Important)

			(3142042) (Critical)			
Windows Server 2012 (Server Core installation)	Not applicable	Not applicable	Windows Server 2012 (Server Core installation) (3145739) (Critical) Microsoft .NET Framework 3.5 (3142043) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Not applicable	Windows Server 2012 (Server Core installation) (3146706) (Important)
Windows Server 2012 R2 (Server Core installation)	Not applicable	Not applicable	Windows Server 2012 R2 (Server Core installation) (3145739) (Critical) Microsoft .NET Framework 3.5 (3142045) (Critical)	Microsoft XML Core Services 3.0 (3146963) (Critical)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3146706) (Important)

Notes for MS16-039

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

Windows Operating Systems and Components (Table 2 of 2)

Windows Vista						
Bulletin Identifier	**MS16-045**	**MS16-046**	**MS16-047**	**MS16-048**	**MS16-049**	**MS16-050**
Aggregate Severity Rating	**None**	**None**	**Important**	**None**	**None**	**None**
Windows Vista Service Pack 2	Not applicable	Not applicable	Windows Vista Service Pack 2 (3149090) (Important)	Not applicable	Not applicable	Not applicable
Windows Vista x64 Edition Service Pack 2	Not applicable	Not applicable	Windows Vista x64 Edition Service Pack 2 (3149090) (Important)	Not applicable	Not applicable	Not applicable
Windows Server 2008						
Bulletin Identifier	**MS16-045**	**MS16-046**	**MS16-047**	**MS16-048**	**MS16-049**	**MS16-050**
Aggregate Severity Rating	**None**	**None**	**Important**	**None**	**None**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2	Not applicable	Not applicable	Windows Server 2008 for	Not applicable	Not applicable	Not applicable

			32-bit Systems Service Pack 2 (3149090) (Important)			
Windows Server 2008 for x64-based Systems Service Pack 2	Not applicable	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3149090) (Important)	Not applicable	Not applicable	Not applicable
Windows Server 2008 for Itanium-based Systems Service Pack 2	Not applicable	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3149090) (Important)	Not applicable	Not applicable	Not applicable
Windows 7						
Bulletin Identifier	**MS16-045**	**MS16-046**	**MS16-047**	**MS16-048**	**MS16-049**	**MS16-050**
Aggregate Severity Rating	**None**	**None**	**Important**	**None**	**None**	**None**
Windows 7 for 32-bit Systems Service Pack 1	Not applicable	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3149090) (Important)	Not applicable	Not applicable	Not applicable
Windows 7 for x64-based Systems Service Pack 1	Not applicable	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3149090) (Important)	Not applicable	Not applicable	Not applicable
Windows Server 2008 R2						
Bulletin Identifier	**MS16-045**	**MS16-046**	**MS16-047**	**MS16-048**	**MS16-049**	**MS16-050**
Aggregate Severity Rating	**None**	**None**	**Important**	**None**	**None**	**None**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1	Not applicable	Not applicable	Not applicable

			(3149090) (Important)			
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3149090) (Important)	Not applicable	Not applicable	Not applicable
Windows 8.1						
Bulletin Identifier	**MS16-045**	**MS16-046**	**MS16-047**	**MS16-048**	**MS16-049**	**MS16-050**
Aggregate Severity Rating	**Important**	**None**	**Important**	**Important**	**None**	**Critical**
Windows 8.1 for 32-bit Systems	Not applicable	Not applicable	Windows 8.1 for 32-bit Systems (3149090) (Important)	Windows 8.1 for 32-bit Systems (3146723) (Important)	Not applicable	Adobe Flash Player (3154132) (Critical)
Windows 8.1 for x64-based Systems	Windows 8.1 for x64-based Systems (3135456) (Important)	Not applicable	Windows 8.1 for x64-based Systems (3149090) (Important)	Windows 8.1 for x64-based Systems (3146723) (Important)	Not applicable	Adobe Flash Player (3154132) (Critical)
Windows Server 2012 and Windows Server 2012 R2						
Bulletin Identifier	**MS16-045**	**MS16-046**	**MS16-047**	**MS16-048**	**MS16-049**	**MS16-050**
Aggregate Severity Rating	**Important**	**None**	**Important**	**Important**	**None**	**Moderate**
Windows Server 2012	Windows Server 2012 (3135456) (Important)	Not applicable	Windows Server 2012 (3149090) (Important)	Windows Server 2012 (3146723) (Important)	Not applicable	Adobe Flash Player (3154132) (Moderate)
Windows Server 2012 R2	Windows Server 2012 R2 (3135456) (Important)	Not applicable	Windows Server 2012 R2 (3149090) (Important)	Windows Server 2012 R2 (3146723) (Important)	Not applicable	Adobe Flash Player (3154132) (Moderate)
Windows RT 8.1						
Bulletin Identifier	**MS16-045**	**MS16-046**	**MS16-047**	**MS16-048**	**MS16-049**	**MS16-050**
Aggregate Severity Rating	**None**	**None**	**Important**	**Important**	**None**	**Critical**
Windows RT 8.1	Not applicable	Not applicable	Windows RT 8.1 (3149090) (Important)	Windows RT 8.1 (3146723) (Important)	Not applicable	Adobe Flash Player (3154132) (Critical)
Windows 10						

Bulletin Identifier	MS16-045	MS16-046	MS16-047	MS16-048	MS16-049	MS16-050
Aggregate Severity Rating	**Important**	**Important**	**Important**	**Important**	**Important**	**Critical**
Windows 10 for 32-bit Systems	Not applicable	Windows 10 for 32-bit Systems (3147461) (Important)	Windows 10 for 32-bit Systems (3147461) (Important)	Windows 10 for 32-bit Systems (3147461) (Important)	Windows 10 for 32-bit Systems (3147461) (Important)	Adobe Flash Player (3154132) (Critical)
Windows 10 for x64-based Systems	Windows 10 for x64-based Systems (3147461) (Important)	Windows 10 for x64-based Systems (3147461) (Important)	Windows 10 for x64-based Systems (3147461) (Important)	Windows 10 for x64-based Systems (3147461) (Important)	Windows 10 for x64-based Systems (3147461) (Important)	Adobe Flash Player (3154132) (Critical)
Windows 10 Version 1511 for 32-bit Systems	Not applicable	Windows 10 Version 1511 for 32-bit Systems (3147458) (Important)	Windows 10 Version 1511 for 32-bit Systems (3147458) (Important)	Windows 10 Version 1511 for 32-bit Systems (3147458) (Important)	Windows 10 Version 1511 for 32-bit Systems (3147458) (Important)	Adobe Flash Player (3154132) (Critical)
Windows 10 Version 1511 for x64-based Systems	Not applicable	Windows 10 Version 1511 for x64-based Systems (3147458) (Important)	Windows 10 Version 1511 for x64-based Systems (3147458) (Important)	Windows 10 Version 1511 for x64-based Systems (3147458) (Important)	Windows 10 Version 1511 for x64-based Systems (3147458) (Important)	Adobe Flash Player (3154132) (Critical)
Server Core installation option						
Bulletin Identifier	**MS16-045**	**MS16-046**	**MS16-047**	**MS16-048**	**MS16-049**	**MS16-050**
Aggregate Severity Rating	**Important**	**None**	**Important**	**Important**	**None**	**None**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3149090) (Important)	Not applicable	Not applicable	Not applicable
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	Not applicable	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3149090) (Important)	Not applicable	Not applicable	Not applicable

Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3149090) (Important)	Not applicable	Not applicable	Not applicable
Windows Server 2012 (Server Core installation)	Windows Server 2012 (Server Core installation) (3135456) (Important)	Not applicable	Windows Server 2012 (Server Core installation) (3149090) (Important)	Windows Server 2012 (Server Core installation) (3146723) (Important)	Not applicable	Not applicable
Windows Server 2012 R2 (Server Core installation)	Windows Server 2012 R2 (Server Core installation) (3135456) (Important)	Not applicable	Windows Server 2012 R2 (Server Core installation) (3149090) (Important)	Windows Server 2012 R2 (Server Core installation) (3146723) (Important)	Not applicable	Not applicable

Microsoft Office Suites and Software

Microsoft Office 2007		
Bulletin Identifier	**MS16-039**	**MS16-042**
Aggregate Severity Rating	**Important**	**Critical**
Microsoft Office 2007 Service Pack 3	Microsoft Office 2007 Service Pack 3 (3114542) (Important)	Microsoft Excel 2007 Service Pack 3 (3114892) (Important) Microsoft Word 2007 Service Pack 3 (3114983) (Critical)
Microsoft Office 2010		
Bulletin Identifier	**MS16-039**	**MS16-042**
Aggregate Severity Rating	**Important**	**Critical**
Microsoft Office 2010 Service Pack 2 (32-bit editions)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3114566) (Important)	Microsoft Office 2010 Service Pack 2 (32-bit editions) (3114990) (Critical) Microsoft Excel 2010 Service Pack 2 (32-bit editions) (3114888) (Important)

		Microsoft Word 2010 Service Pack 2 (32-bit editions) (3114993) (Critical)
Microsoft Office 2010 Service Pack 2 (64-bit editions)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3114566) (Important)	Microsoft Office 2010 Service Pack 2 (64-bit editions) (3114990) (Critical) Microsoft Excel 2010 Service Pack 2 (64-bit editions) (3114888) (Important) Microsoft Word 2010 Service Pack 2 (64-bit editions) (3114993) (Critical)
Microsoft Office 2013		
Bulletin Identifier	**MS16-039**	**MS16-042**
Aggregate Severity Rating	**None**	**Critical**
Microsoft Office 2013 Service Pack 1 (32-bit editions)	Not applicable	Microsoft Excel 2013 Service Pack 1 (32-bit editions) (3114947) (Important) Microsoft Word 2013 Service Pack 1 (32-bit editions) (3114937) (Critical)
Microsoft Office 2013 Service Pack 1 (64-bit editions)	Not applicable	Microsoft Excel 2013 Service Pack 1 (64-bit editions) (3114947) (Important) Microsoft Word 2013 Service Pack 1 (64-bit editions) (3114937) (Critical)
Microsoft Office 2013 RT		
Bulletin Identifier	**MS16-039**	**MS16-042**
Aggregate Severity Rating	**None**	**Critical**
Microsoft Office 2013 RT Service Pack 1	Not applicable	Microsoft Excel 2013 RT Service Pack 1 (3114947) (Important) Microsoft Word 2013 RT Service Pack 1 (3114937) (Critical)
Microsoft Office 2016		
Bulletin Identifier	**MS16-039**	**MS16-042**
Aggregate Severity Rating	**None**	**Important**

Microsoft Office 2016 (32-bit edition)	Not applicable	Microsoft Excel 2016 (32-bit edition) (3114964) (Important)
Microsoft Office 2016 (64-bit edition)	Not applicable	Microsoft Excel 2016 (64-bit edition) (3114964) (Important)
Microsoft Office for Mac 2011		
Bulletin Identifier	**MS16-039**	**MS16-042**
Aggregate Severity Rating	**None**	**Important**
Microsoft Office for Mac 2011	Not applicable	Microsoft Word for Mac 2011 (3154208) (Important)
Microsoft Office 2016 for Mac		
Bulletin Identifier	**MS16-039**	**MS16-042**
Aggregate Severity Rating	**None**	**Important**
Microsoft Office 2016 for Mac	Not applicable	Microsoft Word 2016 for Mac (3142577) (Important)
Other Office Software		
Bulletin Identifier	**MS16-039**	**MS16-042**
Aggregate Severity Rating	**Important**	**Critical**
Microsoft Office Compatibility Pack Service Pack 3	Not applicable	Microsoft Office Compatibility Pack Service Pack 3 (3114982) (Critical) Microsoft Office Compatibility Pack Service Pack 3 (3114895) (Important)
Microsoft Excel Viewer	Not applicable	Microsoft Excel Viewer (3114898) (Important)
Microsoft Word Viewer	Microsoft Word Viewer (3114985) (Important)	Microsoft Word Viewer (3114987) (Critical)

Notes for MS16-039 and MS16-042

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	**MS16-042**
Aggregate Severity Rating	**Important**

Microsoft SharePoint Server 2007 Service Pack 3 (32-bit editions)	Excel Services (3114897) (Important)
Microsoft SharePoint Server 2007 Service Pack 3 (64-bit editions)	Excel Services (3114897) (Important)
Microsoft SharePoint Server 2010	
Bulletin Identifier	**MS16-042**
Aggregate Severity Rating	**Critical**
Microsoft SharePoint Server 2010 Service Pack 2	Excel Services (3114871) (Important) Word Automation Services (3114988) (Critical)
Microsoft SharePoint Server 2013	
Bulletin Identifier	**MS16-042**
Aggregate Severity Rating	**Critical**
Microsoft SharePoint Server 2013 Service Pack 1	Word Automation Services (3114927) (Critical)
Microsoft Office Web Apps 2010	
Bulletin Identifier	**MS16-042**
Aggregate Severity Rating	**Critical**
Microsoft Office Web Apps 2010 Service Pack 2	Microsoft Office Web Apps 2010 Service Pack 2 (3114994) (Critical)
Microsoft Office Web Apps 2013	
Bulletin Identifier	**MS16-042**
Aggregate Severity Rating	**Critical**
Microsoft Office Web Apps Server 2013 Service Pack 1	Microsoft Office Web Apps Server 2013 Service Pack 1 (3114934) (Critical)

Notes for MS16-042

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

Microsoft Communications Platforms and Software

Skype for Business 2016	
Bulletin Identifier	**MS16-039**
Aggregate Severity Rating	**Critical**

Skype for Business 2016 (32-bit editions)	Skype for Business 2016 (32-bit editions) (3114960) (Critical)
Skype for Business Basic 2016 (32-bit editions)	Skype for Business Basic 2016 (32-bit editions) (3114960) (Critical)
Skype for Business 2016 (64-bit editions)	Skype for Business 2016 (64-bit editions) (3114960) (Critical)
Skype for Business Basic 2016 (64-bit editions)	Skype for Business Basic 2016 (64-bit editions) (3114960) (Critical)
Microsoft Lync 2013	
Bulletin Identifier	**MS16-039**
Aggregate Severity Rating	**Critical**
Microsoft Lync 2013 Service Pack 1 (32-bit) (Skype for Business)	Microsoft Lync 2013 Service Pack 1 (32-bit) (Skype for Business) (3114944) (Critical)
Microsoft Lync Basic 2013 Service Pack 1 (32-bit) (Skype for Business Basic)	Microsoft Lync Basic 2013 Service Pack 1 (32-bit) (Skype for Business Basic) (3114944) (Critical)
Microsoft Lync 2013 Service Pack 1 (64-bit) (Skype for Business)	Microsoft Lync 2013 Service Pack 1 (64-bit) (Skype for Business) (3114944) (Critical)
Microsoft Lync Basic 2013 Service Pack 1 (64-bit) (Skype for Business Basic)	Microsoft Lync Basic 2013 Service Pack 1 (64-bit) (Skype for Business Basic) (3114944) (Critical)
Microsoft Lync 2010	
Bulletin Identifier	**MS16-039**
Aggregate Severity Rating	**Critical**
Microsoft Lync 2010 (32-bit)	Microsoft Lync 2010 (32-bit) (3144427) (Critical)
Microsoft Lync 2010 (64-bit)	Microsoft Lync 2010 (64-bit) (3144427) (Critical)
Microsoft Lync 2010 Attendee (user level install)	Microsoft Lync 2010 Attendee (user level install) (3144428) (Critical)
Microsoft Lync 2010 Attendee (admin level install)	Microsoft Lync 2010 Attendee (admin level install) (3144429) (Critical)

Microsoft Live Meeting 2007 Console	
Bulletin Identifier	**MS16-039**
Aggregate Severity Rating	**Critical**
Microsoft Live Meeting 2007 Console	Microsoft Live Meeting 2007 Console (3144432) (Critical)

Notes for MS16-039

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 (April 12, 2016): Bulletin Summary published.
- V1.1 (April 13, 2016): Added a Known Issues reference to the Executive Summaries table for MS16-039. For more information, see Microsoft Knowledge Base Article 3148522. Added a Known Issues reference to the Executive Summaries table for MS16-042. For more information, see Microsoft Knowledge Base Article 3148775.
- V1.2 (May 11, 2016): Added a Known Issues reference to the Executive Summaries table for MS16-044. For more information, see Microsoft Knowledge Base Article 3146706. Added a Known Issues reference to the Executive Summaries table for MS16-042. For more information, see Microsoft Knowledge Base Article 3146723.
- V2.0 (June 14, 2016): For MS16-039, Bulletin Summary revised to announce that Microsoft has re-released security update 3144427 for affected editions of Microsoft Lync 2010 and Microsoft Lync 2010 Attendee. The re-release addresses issues customers might have experienced downloading update 3144427. Customers running Microsoft Lync 2010 should install the update to be fully protected from the vulnerability. See Microsoft Knowledge Base Article 3144427 for more information.
- V3.0 (April 11, 2017): For MS16-037, Bulletin Summary revised to announce the release of a new Internet Explorer cumulative update (4014661) for CVE-2016-0162. The update adds to the original release to comprehensively address CVE-2016-0162. Microsoft recommends that customers running the affected software install the security update to be fully protected from the vulnerability described in this bulletin. See Microsoft Knowledge Base Article 4014661 for more information.
- V4.0 (September 12, 2017): For MS16-039, revised the Windows Operating Systems and Components affected software table to include Windows 10 Version 1703 for 32-bit Systems and Windows 10 Version 1703 for x64-based Systems because they are affected by CVE-2016-0165. Consumers running Windows 10 are automatically protected. Microsoft recommends that enterprise customers running Windows 10 Version 1703 ensure they have update 4038788 installed to be protected from this vulnerability.

Page generated 2017-09-09 17:44-07:00.