Microsoft Security Bulletin Summary for November 2014

Este tema aún no ha recibido ninguna valoración

Published: November 11, 2014 | Updated: November 18, 2014

Version: 2.0

This bulletin summary lists security bulletins released for November 2014.

With the release of the security bulletins for November 2014, this bulletin summary replaces the bulletin advance notification originally issued November 6, 2014. For more information about the bulletin advance notification service, see Microsoft Security Bulletin Advance Notification.

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**.

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	Affected Software
MS14-064	**Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443)** This security update resolves two privately reported vulnerabilities in Microsoft Windows Object Linking and Embedding (OLE). The most severe of these 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 run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Customers 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
MS14-065	**Cumulative Security Update for Internet Explorer (3003057)** This security update resolves seventeen privately reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the current user. 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, Internet Explorer
MS14-066	**Vulnerability in Schannel Could Allow Remote Code Execution (2992611)** This security update resolves a privately reported vulnerability in the Microsoft Secure Channel (Schannel) security package in Windows. The vulnerability could allow remote code execution if an attacker sends specially crafted packets to a Windows server.	Critical Remote Code Execution	Requires restart	Microsoft Windows
MS14-067	**Vulnerability in XML Core Services Could Allow Remote Code Execution (2993958)** This security update resolves a privately reported vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a logged-on user visits a specially crafted website that is designed to invoke Microsoft XML Core Services (MSXML) through Internet Explorer. In all cases, however, an attacker would have no way to force users to visit such websites. Instead, an attacker would have to convince users to visit a website, typically by getting them to click a link in an email message or in an Instant Messenger request that takes users to the attacker's website.	Critical Remote Code Execution	May require restart	Microsoft Windows
MS14-068	**Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780)** This security update resolves a privately reported vulnerability in Microsoft Windows Kerberos KDC that could allow an attacker to elevate unprivileged domain user account privileges to those of the domain administrator account. An attacker could use these elevated privileges to compromise any computer in the domain, including domain controllers. An attacker must have valid domain credentials to exploit this vulnerability. The affected component is available remotely to users who have standard user accounts with domain credentials; this is not the case for users with local account credentials only. When this security bulletin was issued, Microsoft was aware of limited, targeted attacks that attempt to exploit this vulnerability.	Critical Elevation of Privilege	Requires restart	Microsoft Windows
MS14-069	**Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3009710)** This security update resolves three privately reported vulnerabilities in Microsoft Office. The vulnerabilities could	Important Remote Code Execution	May require restart	Microsoft Office

	allow remote code execution if a specially crafted file is opened in an affected edition of Microsoft Office 2007. An attacker who successfully exploited this vulnerability 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.			
MS14-070	**Vulnerability in TCP/IP Could Allow Elevation of Privilege (2989935)** This security update resolves a publically reported vulnerability in TCP/IP that occurs during input/output control (IOCTL) processing. This vulnerability could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application. An attacker who successfully exploited this vulnerability could run arbitrary code in the context of another process. If this process runs with administrator privileges, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Important Elevation of Privilege	May require restart	Microsoft Windows
MS14-071	**Vulnerability in Windows Audio Service Could Allow Elevation of Privilege (3005607)** This security update resolves a privately reported vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an application uses the Microsoft Windows Audio service. The vulnerability by itself does not allow arbitrary code to be run. The vulnerability would have to be used in conjunction with another vulnerability that allowed remote code execution.	Important Elevation of Privilege	Requires restart	Microsoft Windows
MS14-072	**Vulnerability in .NET Framework Could Allow Elevation of Privilege (3005210)** This security update resolves a privately reported vulnerability in Microsoft .NET Framework. The vulnerability could allow elevation of privilege if an attacker sends specially crafted data to an affected workstation or server that uses .NET Remoting. Only custom applications that have been specifically designed to use .NET Remoting would expose a system to the vulnerability.	Important Elevation of Privilege	May require restart	Microsoft Windows, Microsoft .NET Framework
MS14-073	**Vulnerability in Microsoft SharePoint Foundation Could Allow Elevation of Privilege (3000431)** This security update resolves a privately reported vulnerability in Microsoft SharePoint Server. An authenticated attacker who successfully exploited this vulnerability could run arbitrary script in the context of the user on the current SharePoint site. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit these vulnerabilities and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit these vulnerabilities. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by getting them to open an attachment sent through email.	Important Elevation of Privilege	May require restart	Microsoft Server Software
MS14-074	**Vulnerability in Remote Desktop Protocol Could Allow Security Feature Bypass (3003743)** This security update resolves a privately reported vulnerability in Microsoft Windows. The vulnerability could allow security feature bypass when Remote Desktop Protocol (RDP) fails to properly log audit events. By default, RDP is not enabled on any Windows operating system. Systems that do not have RDP enabled are not at risk.	Important Security Feature Bypass	Requires restart	Microsoft Windows
MS14-075	Release date to be determined			
MS14-076	**Vulnerability in Internet Information Services (IIS) Could Allow Security Feature Bypass (2982998)** This security update resolves a privately reported vulnerability in Microsoft Internet Information Services (IIS) that could lead to a bypass of the "IP and domain restrictions" security feature. Successful exploitation of this vulnerability could result in clients from restricted or blocked domains having access to restricted web resources.	Important Security Feature Bypass	May require restart	Microsoft Windows
MS14-077	**Vulnerability in Active Directory Federation Services Could Allow Information Disclosure (3003381)** This security update resolves a privately reported vulnerability in Active Directory Federation Services (AD FS). The vulnerability could allow information disclosure if a user leaves their browser open after logging off from an application, and an attacker reopens the application in the browser immediately after the user has logged off.	Important Information Disclosure	May require restart	Microsoft Windows
MS14-078	**Vulnerability in IME (Japanese) Could Allow Elevation of Privilege (2992719)** This security update resolves a privately reported vulnerability in Microsoft Input Method Editor (IME) (Japanese). The vulnerability could allow sandbox escape based on the application sandbox policy on a system where an affected version of the Microsoft IME (Japanese) is installed. An attacker who successfully exploited this vulnerability could escape the sandbox of a vulnerable application and gain access to the affected system with logged-in user rights. If the affected system is logged in with administrative rights, an attacker could then install programs; view, change or delete data; or create new accounts with full administrative rights.	Moderate Elevation of Privilege	May require restart	Microsoft Windows, Microsoft Office
MS14-079	**Vulnerability in Kernel Mode Driver Could Allow Denial of Service (3002885)** This security update resolves a privately reported vulnerability in Microsoft Windows. The vulnerability could allow denial of service if an attacker places a specially crafted TrueType font on a network share and a user subsequently navigates there in Windows Explorer. In a web-based attack scenario, an attacker could host a website that contains a webpage that is used to exploit this vulnerability. In addition, compromised websites and websites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit such websites. Instead, an attacker would have to persuade users to visit a website, typically by getting them to click a link in an email message or Instant Messenger message that takes them to the attacker's website.	Moderate Denial of Service	Requires restart	Microsoft Windows

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.

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.

Bulletin ID	Vulnerability Title	CVE ID	Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment	Key Notes
MS14-064	Windows OLE Automation Array Remote Code Execution Vulnerability	CVE-2014-6332	1- Exploitation More Likely	1- Exploitation More Likely	Not Applicable	(None)
MS14-064	Windows OLE Remote Code Execution Vulnerability	CVE-2014-6352	0- Exploitation Detected	0- Exploitation Detected	Not Applicable	Microsoft is aware of limited attacks that attempt to exploit this vulnerability. This vulnerability was first described in Microsoft Security Advisory 3010060.
MS14-065	Internet Explorer Memory Corruption Vulnerability	CVE-2014-4143	1- Exploitation More Likely	1- Exploitation More Likely	Not Applicable	(None)
MS14-065	Internet Explorer Clipboard Information Disclosure Vulnerability	CVE-2014-6323	1- Exploitation More Likely	1- Exploitation More Likely	Not Applicable	This is an information disclosure vulnerability.
MS14-065	Internet Explorer Memory Corruption Vulnerability	CVE-2014-6337	1- Exploitation More Likely	1- Exploitation More Likely	Not Applicable	(None)
MS14-065	Internet Explorer ASLR Bypass Vulnerability	CVE-2014-6339	Not Affected	1- Exploitation More Likely	Not Applicable	This is a security feature bypass vulnerability.
MS14-065	Internet Explorer Cross-domain Information Disclosure Vulnerability	CVE-2014-6340	2- Exploitation Less Likely	2- Exploitation Less Likely	Not Applicable	This is an information disclosure vulnerability.
MS14-065	Internet Explorer Memory Corruption Vulnerability	CVE-2014-6341	1- Exploitation More Likely	1- Exploitation More Likely	Not Applicable	(None)
MS14-065	Internet Explorer Memory Corruption Vulnerability	CVE-2014-6342	Not Affected	1- Exploitation More Likely	Not Applicable	(None)
MS14-065	Internet Explorer Memory Corruption Vulnerability	CVE-2014-6343	1- Exploitation More Likely	1- Exploitation More Likely	Not Applicable	(None)
MS14-065	Internet Explorer Memory Corruption Vulnerability	CVE-2014-6344	Not Affected	1- Exploitation More Likely	Not Applicable	(None)
MS14-065	Internet Explorer Cross-domain Information Disclosure Vulnerability	CVE-2014-6345	Not Affected	2- Exploitation Less Likely	Not Applicable	This is an information disclosure vulnerability.
MS14-065	Internet Explorer Cross-domain Information Disclosure Vulnerability	CVE-2014-6346	2- Exploitation Less Likely	2- Exploitation Less Likely	Not Applicable	This is an information disclosure vulnerability.
MS14-065	Internet Explorer Memory Corruption Vulnerability	CVE-2014-6347	1- Exploitation More Likely	Not Affected	Not Applicable	(None)
MS14-065	Internet Explorer Memory Corruption Vulnerability	CVE-2014-6348	Not Affected	1- Exploitation More Likely	Not Applicable	(None)
MS14-065	Internet Explorer Elevation of Privilege Vulnerability	CVE-2014-6349	1- Exploitation More Likely	1- Exploitation More Likely	Not Applicable	This is an elevation of privilege vulnerability.

MS14-065	Internet Explorer Elevation of Privilege Vulnerability	CVE-2014-6350	1- Exploitation More Likely	1- Exploitation More Likely	Not Applicable	This is an elevation of privilege vulnerability.
MS14-065	Internet Explorer Memory Corruption Vulnerability	CVE-2014-6351	1- Exploitation More Likely	1- Exploitation More Likely	Not Applicable	(None)
MS14-065	Internet Explorer Memory Corruption Vulnerability	CVE-2014-6353	Not Affected	1- Exploitation More Likely	Not Applicable	(None)
MS14-066	Microsoft Schannel Remote Code Execution Vulnerability	CVE-2014-6321	1- Exploitation More Likely	1- Exploitation More Likely	Permanent	(None)
MS14-067	MSXML Remote Code Execution Vulnerability	CVE-2014-4118	2- Exploitation Less Likely	2- Exploitation Less Likely	Not Applicable	(None)
MS14-068	Kerberos Checksum Vulnerability	CVE-2014-6324	1- Exploitation More Likely	0- Exploitation Detected	Not Applicable	This is an elevation of privilege vulnerability. Microsoft is aware of limited, targeted attacks that attempt to exploit this vulnerability.
MS14-069	Microsoft Office Double Delete Remote Code Execution Vulnerability	CVE-2014-6333	Not Affected	2- Exploitation Less Likely	Not Applicable	(None)
MS14-069	Microsoft Office Bad Index Remote Code Execution Vulnerability	CVE-2014-6334	Not Affected	2- Exploitation Less Likely	Not Applicable	(None)
MS14-069	Microsoft Office Invalid Pointer Remote Code Execution Vulnerability	CVE-2014-6335	Not Affected	1- Exploitation More Likely	Not Applicable	(None)
MS14-070	TCP/IP Elevation of Privilege Vulnerability	CVE-2014-4076	Not Affected	2- Exploitation Less Likely	Permanent	This is an elevation of privilege vulnerability.
MS14-071	Windows Audio Service Vulnerability	CVE-2014-6322	2- Exploitation Less Likely	2- Exploitation Less Likely	Not Applicable	This is an elevation of privilege vulnerability.
MS14-072	TypeFilterLevel Vulnerability	CVE-2014-4149	2- Exploitation Less Likely	2- Exploitation Less Likely	Not Applicable	This is an elevation of privilege vulnerability.
MS14-073	SharePoint Elevation of Privilege Vulnerability	CVE-2014-4116	Not Affected	2- Exploitation Less Likely	Not Applicable	This is an elevation of privilege vulnerability.
MS14-074	Remote Desktop Protocol (RDP) Failure to Audit Vulnerability	CVE-2014-6318	3- Exploitation Unlikely	3- Exploitation Unlikely	Not Applicable	This is a security feature bypass vulnerability.
MS14-076	IIS Security Feature Bypass Vulnerability	CVE-2014-4078	3- Exploitation Unlikely	3- Exploitation Unlikely	Not Applicable	This is a security feature bypass vulnerability.
MS14-077	Active Directory Federation Services Information Disclosure Vulnerability	CVE-2014-6331	3- Exploitation Unlikely	3- Exploitation Unlikely	Not Applicable	This is an information disclosure vulnerability.
MS14-078	Microsoft IME (Japanese) Elevation of Privilege Vulnerability	CVE-2014-4077	Not Affected	0- Exploitation Detected	Not Applicable	This is an elevation of privilege vulnerability.
MS14-079	Denial of Service in Windows Kernel Mode Driver Vulnerability	CVE-2014-6317	3- Exploitation Unlikely	3- Exploitation Unlikely	Permanent	This is a denial of service vulnerability.

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 System and Components

Windows Server 2003												
Bulletin Identifier	**MS14-064**	**MS14-065**	**MS14-066**	**MS14-067**	**MS14-068**	**MS14-070**	**MS14-071**	**MS14-072**	**MS14-074**	**MS14-076**	**MS14-077**	**I**
Aggregate Severity Rating	**Critical**	**Moderate**	**Critical**	**Important**	**Critical**	**Important**	**None**	**Important**	**None**	**None**	**None**	**I**
Windows Server 2003 Service Pack 2	Windows Server 2003 Service Pack 2 (3006226) (Critical)	Internet Explorer 6 (3003057) (Moderate) Internet Explorer 7 (3003057) (Moderate) Internet Explorer 8 (3003057) (Moderate)	Windows Server 2003 Service Pack 2 (2992611) (Critical)	Windows Server 2003 Service Pack 2 (2993958) (Important)	Windows Server 2003 Service Pack 2 (3011780) (Critical)	Windows Server 2003 Service Pack 2 (2989935) (Important)	Not applicable	Microsoft .NET Framework 1.1 Service Pack 1 (2978114) (Important) Microsoft .NET Framework 2.0 Service Pack 2 (2978124) (Important) Microsoft .NET Framework 4 (2978125) (Important)	Not applicable	Not applicable	Not applicable	\ S 2 S F ((
Windows Server 2003 x64 Edition Service Pack 2	Windows Server 2003 x64 Edition Service Pack 2 (3006226) (Critical)	Internet Explorer 6 (3003057) (Moderate) Internet Explorer 7 (3003057) (Moderate) Internet Explorer 8 (3003057) (Moderate)	Windows Server 2003 x64 Edition Service Pack 2 (2992611) (Critical)	Windows Server 2003 x64 Edition Service Pack 2 (2993958) (Important)	Windows Server 2003 x64 Edition Service Pack 2 (3011780) (Critical)	Windows Server 2003 x64 Edition Service Pack 2 (2989935) (Important)	Not applicable	Microsoft .NET Framework 2.0 Service Pack 2 (2978124) (Important) Microsoft .NET Framework 4 (2978125) (Important)	Not applicable	Not applicable	Not applicable	\ S 2 E S F ((
Windows Server 2003 with SP2 for Itanium-based Systems	Windows Server 2003 with SP2 for Itanium-based Systems (3006226) (Critical)	Internet Explorer 6 (3003057) (Moderate) Internet Explorer 7 (3003057) (Moderate)	Windows Server 2003 with SP2 for Itanium-based Systems (2992611) (Critical)	Windows Server 2003 with SP2 for Itanium-based Systems (2993958) (Important)	Windows Server 2003 with SP2 for Itanium-based Systems (3011780) (Critical)	Windows Server 2003 with SP2 for Itanium-based Systems (2989935) (Important)	Not applicable	Microsoft .NET Framework 2.0 Service Pack 2 (2978124) (Important) Microsoft .NET Framework 4 (2978125) (Important)	Not applicable	Not applicable	Not applicable	\ S 2 S I b S ((

Windows Vista												
Bulletin Identifier	**MS14-064**	**MS14-065**	**MS14-066**	**MS14-067**	**MS14-068**	**MS14-070**	**MS14-071**	**MS14-072**	**MS14-074**	**MS14-076**	**MS14-077**	**I**
Aggregate	**Critical**	**Critical**	**Critical**	**Critical**	**None**	**None**	**Important**	**Important**	**Important**	**None**	**None**	**I**

Severity Rating											
Windows Vista Service Pack 2	Windows Vista Service Pack 2 (3006226) (Critical) Windows Vista Service Pack 2 (3010788) (Important)	Internet Explorer 7 (3003057) (Critical) Internet Explorer 8 (3003057) (Critical) Internet Explorer 9 (3003057) (Critical)	Windows Vista Service Pack 2 (2992611) (Critical)	Windows Vista Service Pack 2 (2993958) (Critical)	Windows Vista Service Pack 2 (3011780) (No severity rating)[1]	Not applicable	Windows Vista Service Pack 2 (3005607) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (2978116) (Important) Microsoft .NET Framework 4 (2978125) (Important) Microsoft .NET Framework 4.5/4.5.1/4.5.2 (2978128) (Important)	Windows Vista Service Pack 2 (3003743) (Important)	Not applicable	Not applicable
Windows Vista x64 Edition Service Pack 2	Windows Vista x64 Edition Service Pack 2 (3006226) (Critical) Windows Vista x64 Edition Service Pack 2 (3010788) (Important)	Internet Explorer 7 (3003057) (Critical) Internet Explorer 8 (3003057) (Critical) Internet Explorer 9 (3003057) (Critical)	Windows Vista x64 Edition Service Pack 2 (2992611) (Critical)	Windows Vista x64 Edition Service Pack 2 (2993958) (Critical)	Windows Vista x64 Edition Service Pack 2 (3011780) (No severity rating)[1]	Not applicable	Windows Vista x64 Edition Service Pack 2 (3005607) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (2978116) (Important) Microsoft .NET Framework 4 (2978125) (Important) Microsoft .NET Framework 4.5/4.5.1/4.5.2 (2978128) (Important)	Windows Vista x64 Edition Service Pack 2 (3003743) (Important)	Not applicable	Not applicable
Windows Server 2008											
Bulletin Identifier	**MS14-064**	**MS14-065**	**MS14-066**	**MS14-067**	**MS14-068**	**MS14-070**	**MS14-071**	**MS14-072**	**MS14-074**	**MS14-076**	**MS14-077**
Aggregate Severity Rating	**Critical**	**Moderate**	**Critical**	**Important**	**Critical**	**None**	**Important**	**Important**	**Important**	**None**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2	Windows Server 2008 for 32-bit Systems Service Pack 2 (3006226) (Critical) Windows Server 2008 for 32-bit Systems Service Pack 2 (3010788) (Important)	Internet Explorer 7 (3003057) (Moderate) Internet Explorer 8 (3003057) (Moderate) Internet Explorer 9 (3003057) (Moderate)	Windows Server 2008 for 32-bit Systems Service Pack 2 (2992611) (Critical)	Windows Server 2008 for 32-bit Systems Service Pack 2 (2993958) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3011780) (Critical)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (3005607) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (2978116) (Important) Microsoft .NET Framework 4 (2978125) (Important) Microsoft .NET Framework 4.5/4.5.1/4.5.2 (2978128) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (3003743) (Important)	Not applicable	Active Directory Federation Services 2.0 (3003381) (Important)
Windows Server 2008 for x64-based Systems Service Pack 2	Windows Server 2008 for x64-based Systems Service Pack 2 (3006226) (Critical)	Internet Explorer 7 (3003057) (Moderate) Internet Explorer 8 (3003057) (Moderate)	Windows Server 2008 for x64-based Systems Service Pack 2 (2992611) (Critical)	Windows Server 2008 for x64-based Systems Service Pack 2 (2993958) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (3011780) (Critical)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (3005607) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (2978116) (Important) Microsoft .NET	Windows Server 2008 for x64-based Systems Service Pack 2 (3003743) (Important)	Not applicable	Active Directory Federation Services 2.0 (3003381) (Important)

	Windows Server 2008 for x64-based Systems Service Pack 2 (3010788) (Important)	Internet Explorer 9 (3003057) (Moderate)						Framework 4 (2978125) (Important) Microsoft .NET Framework 4.5/4.5.1/4.5.2 (2978128) (Important)			
Windows Server 2008 for Itanium-based Systems Service Pack 2	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3006226) (Critical) Windows Server 2008 for Itanium-based Systems Service Pack 2 (3010788) (Important)	Internet Explorer 7 (3003057) (Moderate)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (2992611) (Critical)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (2993958) (Important)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3011780) (Critical)	Not applicable	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3005607) (Important)	Microsoft .NET Framework 2.0 Service Pack 2 (2978116) (Important) Microsoft .NET Framework 4 (2978125) (Important)	Windows Server 2008 for Itanium-based Systems Service Pack 2 (3003743) (Important)	Not applicable	Not applicable
Windows 7											
Bulletin Identifier	**MS14-064**	**MS14-065**	**MS14-066**	**MS14-067**	**MS14-068**	**MS14-070**	**MS14-071**	**MS14-072**	**MS14-074**	**MS14-076**	**MS14-077**
Aggregate Severity Rating	**Critical**	**Critical**	**Critical**	**Critical**	**None**	**None**	**Important**	**Important**	**Important**	**None**	**None**
Windows 7 for 32-bit Systems Service Pack 1	Windows 7 for 32-bit Systems Service Pack 1 (3006226) (Critical) Windows 7 for 32-bit Systems Service Pack 1 (3010788) (Important)	Internet Explorer 8 (3003057) (Critical) Internet Explorer 9 (3003057) (Critical) Internet Explorer 10 (3003057) (Critical) Internet Explorer 11 (3003057) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (2992611) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (2993958) (Critical)	Windows 7 for 32-bit Systems Service Pack 1 (3011780) (No severity rating)[1]	Not applicable	Windows 7 for 32-bit Systems Service Pack 1 (3005607) (Important)	Microsoft .NET Framework 3.5.1 (2978120) (Important) Microsoft .NET Framework 4 (2978125) (Important) Microsoft .NET Framework 4.5/4.5.1/4.5.2 (2978128) (Important)	Windows 7 for 32-bit Systems Service Pack 1 (3003743) (Important)	Not applicable	Not applicable
Windows 7 for x64-based Systems Service Pack 1	Windows 7 for x64-based Systems Service Pack 1 (3006226) (Critical) Windows 7 for x64-based Systems Service Pack 1 (3010788) (Important)	Internet Explorer 8 (3003057) (Critical) Internet Explorer 9 (3003057) (Critical) Internet Explorer 10 (3003057) (Critical) Internet Explorer 11 (3003057)	Windows 7 for x64-based Systems Service Pack 1 (2992611) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (2993958) (Critical)	Windows 7 for x64-based Systems Service Pack 1 (3011780) (No severity rating)[1]	Not applicable	Windows 7 for x64-based Systems Service Pack 1 (3005607) (Important)	Microsoft .NET Framework 3.5.1 (2978120) (Important) Microsoft .NET Framework 4 (2978125) (Important) Microsoft .NET Framework 4.5/4.5.1/4.5.2 (2978128) (Important)	Windows 7 for x64-based Systems Service Pack 1 (3003743) (Important)	Not applicable	Not applicable

		(Critical)										
Windows Server 2008 R2												
Bulletin Identifier	**MS14-064**	**MS14-065**	**MS14-066**	**MS14-067**	**MS14-068**	**MS14-070**	**MS14-071**	**MS14-072**	**MS14-074**	**MS14-076**	**MS14-077**	**I**
Aggregate Severity Rating	**Critical**	**Moderate**	**Critical**	**Important**	**Critical**	**None**	**Important**	**Important**	**Important**	**None**	**Important**	**I**
Windows Server 2008 R2 for x64-based Systems Service Pack 1	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3006226) (Critical) Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3010788) (Important)	Internet Explorer 8 (3003057) (Moderate) Internet Explorer 9 (3003057) (Moderate) Internet Explorer 10 (3003057) (Moderate) Internet Explorer 11 (3003057) (Moderate)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (2992611) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (2993958) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3011780) (Critical)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3005607) (Important)	Microsoft .NET Framework 3.5.1 (2978120) (Important) Microsoft .NET Framework 4 (2978125) (Important) Microsoft .NET Framework 4.5/4.5.1/4.5.2 (2978128) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (3003743) (Important)	Not applicable	Active Directory Federation Services 2.0 (3003381) (Important)	\ S 2 › S S F ((
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3006226) (Critical) Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3010788) (Important)	Internet Explorer 8 (3003057) (Moderate)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (2992611) (Critical)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (2993958) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3011780) (Critical)	Not applicable	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3005607) (Important)	Microsoft .NET Framework 3.5.1 (2978120) (Important) Microsoft .NET Framework 4 (2978125) (Important)	Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (3003743) (Important)	Not applicable	Not applicable	\ S 2 I k S S F ((
Windows 8 and Windows 8.1												
Bulletin Identifier	**MS14-064**	**MS14-065**	**MS14-066**	**MS14-067**	**MS14-068**	**MS14-070**	**MS14-071**	**MS14-072**	**MS14-074**	**MS14-076**	**MS14-077**	**I**
Aggregate Severity Rating	**Critical**	**Critical**	**Critical**	**Critical**	**None**	**None**	**Important**	**Important**	**Important**	**Important**	**None**	**I**
Windows 8 for 32-bit Systems	Windows 8 for 32-bit Systems (3006226) (Critical) Windows 8 for 32-bit Systems (3010788) (Important)	Internet Explorer 10 (3003057) (Critical)	Windows 8 for 32-bit Systems (2992611) (Critical)	Windows 8 for 32-bit Systems (2993958) (Critical)	Windows 8 for 32-bit Systems (3011780) (No severity rating)[1]	Not applicable	Windows 8 for 32-bit Systems (3005607) (Important)	Microsoft .NET Framework 3.5 (2978121) (Important) Microsoft .NET Framework 4.5/4.5.1/4.5.2 (2978127) (Important)	Windows 8 for 32-bit Systems (3003743) (Important)	Microsoft Internet Information Services 8.0 (2982998) (Important)	Not applicable	I a
Windows 8 for x64-based Systems	Windows 8 for x64-based Systems (3006226)	Internet Explorer 10 (3003057) (Critical)	Windows 8 for x64-based Systems (2992611)	Windows 8 for x64-based Systems (2993958)	Windows 8 for x64-based Systems (3011780)	Not applicable	Windows 8 for x64-based Systems (3005607)	Microsoft .NET Framework 3.5 (2978121)	Windows 8 for x64-based Systems (3003743)	Microsoft Internet Information Services 8.0 (2982998)	Not applicable	I a

	(Critical) Windows 8 for x64-based Systems (3010788) (Important)		(Critical)	(Critical)	(No severity rating)[1]		(Important)	(Important) Microsoft .NET Framework 4.5/4.5.1/4.5.2 (2978127) (Important)	(Important)	(Important)		
Windows 8.1 for 32-bit Systems	Windows 8.1 for 32-bit Systems (3006226) (Critical) Windows 8.1 for 32-bit Systems (3010788) (Important)	Internet Explorer 11 (3003057) (Critical)	Windows 8.1 for 32-bit Systems (2992611) (Critical)	Windows 8.1 for 32-bit Systems (2993958) (Critical)	Windows 8.1 for 32-bit Systems (3011780) (No severity rating)[1]	Not applicable	Windows 8.1 for 32-bit Systems (3005607) (Important)	Microsoft .NET Framework 3.5 (2978122) (Important) Microsoft .NET Framework 4.5.1/4.5.2 (2978126) (Important)	Windows 8.1 for 32-bit Systems (3003743) (Important)	Microsoft Internet Information Services 8.5 (2982998) (Important)	Not applicable	I a
Windows 8.1 for x64-based Systems	Windows 8.1 for x64-based Systems (3006226) (Critical) Windows 8.1 for x64-based Systems (3010788) (Important)	Internet Explorer 11 (3003057) (Critical)	Windows 8.1 for x64-based Systems (2992611) (Critical)	Windows 8.1 for x64-based Systems (2993958) (Critical)	Windows 8.1 for x64-based Systems (3011780) (No severity rating)[1]	Not applicable	Windows 8.1 for x64-based Systems (3005607) (Important)	Microsoft .NET Framework 3.5 (2978122) (Important) Microsoft .NET Framework 4.5.1/4.5.2 (2978126) (Important)	Windows 8.1 for x64-based Systems (3003743) (Important)	Microsoft Internet Information Services 8.5 (2982998) (Important)	Not applicable	I a
Windows Server 2012 and Windows Server 2012 R2												
Bulletin Identifier	**MS14-064**	**MS14-065**	**MS14-066**	**MS14-067**	**MS14-068**	**MS14-070**	**MS14-071**	**MS14-072**	**MS14-074**	**MS14-076**	**MS14-077**	**I**
Aggregate Severity Rating	**Critical**	**Moderate**	**Critical**	**Important**	**Critical**	**None**	**Important**	**Important**	**Important**	**Important**	**Important**	**I**
Windows Server 2012	Windows Server 2012 (3006226) (Critical) Windows Server 2012 (3010788) (Important)	Internet Explorer 10 (3003057) (Moderate)	Windows Server 2012 (2992611) (Critical)	Windows Server 2012 (2993958) (Important)	Windows Server 2012 (3011780) (Critical)	Not applicable	Windows Server 2012 (3005607) (Important)	Microsoft .NET Framework 3.5 (2978121) (Important) Microsoft .NET Framework 4.5/4.5.1/4.5.2 (2978127) (Important)	Windows Server 2012 (3003743) (Important)	Microsoft Internet Information Services 8.0 (2982998) (Important)	Active Directory Federation Services 2.1 (3003381) (Important)	I a
Windows Server 2012 R2	Windows Server 2012 R2 (3006226) (Critical) Windows Server 2012 R2 (3010788) (Important)	Internet Explorer 11 (3003057) (Moderate)	Windows Server 2012 R2 (2992611) (Critical)	Windows Server 2012 R2 (2993958) (Important)	Windows Server 2012 R2 (3011780) (Critical)	Not applicable	Windows Server 2012 R2 (3005607) (Important)	Microsoft .NET Framework 3.5 (2978122) (Important) Microsoft .NET Framework 4.5.1/4.5.2 (2978126) (Important)	Windows Server 2012 R2 (3003743) (Important)	Microsoft Internet Information Services 8.5 (2982998) (Important)	Active Directory Federation Services 3.0 (3003381) (Important)	I a
Windows RT and Windows RT 8.1												
Bulletin Identifier	**MS14-064**	**MS14-065**	**MS14-066**	**MS14-067**	**MS14-068**	**MS14-070**	**MS14-071**	**MS14-072**	**MS14-074**	**MS14-076**	**MS14-077**	**I**
Aggregate Severity Rating	**Critical**	**Critical**	**Critical**	**Critical**	**None**	**None**	**Important**	**Important**	**Important**	**None**	**None**	**I**
Windows	Windows	Internet	Windows	Windows	Not	Not	Windows	Microsoft	Windows	Not	Not	I

RT	RT (3006226) (Critical) Windows RT (3010788) (Important)	Explorer 10 (3003057) (Critical)	RT (2992611) (Critical)	RT (2993958) (Critical)	applicable	applicable	RT (3005607) (Important)	.NET Framework 4.5/4.5.1/4.5.2 (2978127) (Important)	RT (3003743) (Important)	applicable	applicable
Windows RT 8.1	Windows RT 8.1 (3006226) (Critical) Windows RT 8.1 (3010788) (Important)	Internet Explorer 11 (3003057) (Critical)	Windows RT 8.1 (2992611) (Critical)	Windows RT 8.1 (2993958) (Critical)	Not applicable	Not applicable	Windows RT 8.1 (3005607) (Important)	Microsoft .NET Framework 4.5.1/4.5.2 (2978126) (Important)	Windows RT 8.1 (3003743) (Important)	Not applicable	Not applicable
Server Core installation option											
Bulletin Identifier	**MS14-064**	**MS14-065**	**MS14-066**	**MS14-067**	**MS14-068**	**MS14-070**	**MS14-071**	**MS14-072**	**MS14-074**	**MS14-076**	**MS14-077**
Aggregate Severity Rating	**Critical**	**None**	**Critical**	**Important**	**Critical**	**None**	**None**	**Important**	**Important**	**None**	**Important**
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3006226) (Critical)	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (2992611) (Critical)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (2993958) (Important)	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3011780) (Critical)	Not applicable	Not applicable	Not applicable	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) (3003743) (Important)	Not applicable	Not applicable
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) (3006226) (Critical)	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (2992611) (Critical)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (2993958) (Important)	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3011780) (Critical)	Not applicable	Not applicable	Not applicable	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) (3003743) (Important)	Not applicable	Not applicable
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) (3006226) (Critical)	Not applicable	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (2992611) (Critical)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (2993958) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3011780) (Critical)	Not applicable	Not applicable	Microsoft .NET Framework 3.5.1 (2978120) (Important) Microsoft .NET Framework 4 (2978125) (Important) Microsoft .NET Framework 4.5/4.5.1/4.5.2 (2978128) (Important)	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) (3003743) (Important)	Not applicable	Not applicable
Windows Server 2012 (Server Core installation)	Windows Server 2012 (Server Core installation) (3006226) (Critical)	Not applicable	Windows Server 2012 (Server Core installation) (2992611) (Critical)	Windows Server 2012 (Server Core installation) (2993958) (Important)	Windows Server 2012 (Server Core installation) (3011780) (Critical)	Not applicable	Not applicable	Microsoft .NET Framework 3.5 (2978121) (Important) Microsoft .NET Framework	Windows Server 2012 (Server Core installation) (3003743) (Important)	Not applicable	Not applicable

								4.5/4.5.1/4.5.2 (2978127) (Important)				
Windows Server 2012 R2 (Server Core installation)	Windows Server 2012 R2 (Server Core installation) (3006226) (Critical)	Not applicable	Windows Server 2012 R2 (Server Core installation) (2992611) (Critical)	Windows Server 2012 R2 (Server Core installation) (2993958) (Important)	Windows Server 2012 R2 (Server Core installation) (3011780) (Critical)	Not applicable	Not applicable	Microsoft .NET Framework 3.5 (2978122) (Important) Microsoft .NET Framework 4.5.1/4.5.2 (2978126) (Important)	Windows Server 2012 R2 (Server Core installation) (3003743) (Important)	Not applicable	Active Directory Federation Services 3.0 (3003381) (Important)

Note for MS14-064, MS14-065, and MS14-067

Windows Technical Preview and Windows Server Technical Preview are affected. Customers running these operating systems are encouraged to apply the update, which is available via Windows Update.

Notes for MS14-068

Windows Technical Preview and Windows Server Technical Preview are affected. Customers running these operating systems are encouraged to apply the update, which is available via Windows Update.

[1]Severity ratings do not apply for this operating system because the vulnerability addressed in this bulletin is not present. This update provides additional defense-in-depth hardening that does not fix any known vulnerability.

Note for MS14-078

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

Microsoft Office Suites and Software

Microsoft Office 2007		
Bulletin Identifier	**MS14-069**	**MS14-078**
Aggregate Severity Rating	**Important**	**Moderate**
Microsoft Office 2007 Service Pack 3	Microsoft Word 2007 Service Pack 3 (2899527) (Important)	Microsoft Office 2007 IME (Japanese) (2889913) (Moderate)
Other Microsoft Office Software		
Bulletin Identifier	**MS14-069**	**MS14-078**
Aggregate Severity Rating	**Important**	**None**
Microsoft Word Viewer	Microsoft Word Viewer (2899553) (Important)	Not applicable
Microsoft Office Compatibility Pack Service Pack 3	Microsoft Office Compatibility Pack Service Pack 3 (2899526) (Important)	Not applicable

Note for MS14-078

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 2010	
Bulletin Identifier	**MS14-073**
Aggregate Severity Rating	**Important**
Microsoft SharePoint Server 2010 Service Pack 2	Microsoft SharePoint Foundation 2010 Service Pack 2 (2889838) (Important)

Detection and Deployment Tools and Guidance

Several resources are available to help administrators deploy security updates.

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

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

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

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

Acknowledgments

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

Other Information

Microsoft Windows Malicious Software Removal Tool

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

Non-Security Updates on MU, WU, and WSUS

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

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

Microsoft Active Protections Program (MAPP)

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

Security Strategies and Community

Update Management Strategies

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

Obtaining Other Security Updates

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

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

IT Pro Security Community

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

Support

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

Security solutions for IT professionals: TechNet Security Troubleshooting and Support

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

Local support according to your country: International Support

Disclaimer

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

Revisions

- V1.0 (November 11, 2014): Bulletin Summary published.
- V2.0 (November 18, 2014): Bulletin Summary revised to document the out-of-band release of MS14-068 and, for MS14-066, to announce the reoffering of the 2992611 update to systems running Windows Server 2008 R2 and Windows Server 2012.

Page generated 2014-11-18 6:52Z-08:00.

¿Te ha resultado útil? ○ Sí ○ No