Microsoft Security Bulletin Advance Notification for September 2010

Published: September 09, 2010

Microsoft Security Bulletin Advance Notification issued: September 9, 2010
Microsoft Security Bulletins to be issued: September 14, 2010

This is an advance notification of security bulletins that Microsoft is intending to release on September 14, 2010.

This bulletin advance notification will be replaced with the September bulletin summary on September 14, 2010. For more information about the bulletin advance notification service, see Microsoft Security Bulletin Advance Notification.

To receive automatic notifications whenever Microsoft Security Bulletins are issued, subscribe to Microsoft Technical Security Notifications.

Microsoft will host a webcast to address customer questions on these bulletins on September 15, 2010, at 11:00 AM Pacific Time (US & Canada). Register now for the September Security Bulletin Webcast. After this date, this webcast is available on-demand. For more information, see Microsoft Security Bulletin Summaries and Webcasts.

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

Bulletin Information

Executive Summaries

This advance notification provides a number as the bulletin identifier, because the official Microsoft Security Bulletin numbers are not issued until release. The bulletin summary that replaces this advance notification will have the proper Microsoft Security Bulletin numbers (in the MS*yy-xxx* format) as the bulletin identifier.

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	Maximum Severity Rating and Vulnerability Impact	Restart Requirement	Affected Software
Bulletin 1	Critical Remote Code Execution	Requires restart	Microsoft Windows
Bulletin 2	Critical Remote Code Execution	May require restart	Microsoft Windows
Bulletin 3	Critical Remote Code Execution	May require restart	Microsoft Windows, Microsoft Office
Bulletin 4	Critical Remote Code Execution	May require restart	Microsoft Office
Bulletin 5	Important Remote Code Execution	May require restart	Microsoft Windows
Bulletin 6	Important Remote Code Execution	Requires restart	Microsoft Windows
Bulletin 7	Important Remote Code Execution	May require restart	Microsoft Windows
Bulletin 8	Important Elevation of Privilege	Requires restart	Microsoft Windows
Bulletin 9	Important Elevation of Privilege	Requires restart	Microsoft Windows

Top of section

Affected Software

This advance notification provides a number as the bulletin identifier, because the official Microsoft Security Bulletin numbers are not issued until release. The bulletin summary that replaces this advance notification will have the proper Microsoft Security Bulletin numbers (in the MS*yy-xxx* format) as the bulletin identifier.

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

How do I use these tables?

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 security 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 XP								
Bulletin Identifier	**Bulletin 1**	**Bulletin 2**	**Bulletin 3**	**Bulletin 5**	**Bulletin 6**	**Bulletin 7**	**Bulletin 8**	**Bulletin 9**
Aggregate Severity Rating	Critical	Critical	Critical	Important	Important	Important	Important	Important
Windows XP Service Pack 3	Windows XP Service Pack 3 (Critical)	Windows XP Service Pack 3 (Critical)	Windows XP Service Pack 3 (Critical)	Windows XP Service Pack 3 (Important)	Windows XP Service Pack 3 (Important)	Windows XP Service Pack 3 (Important)	Windows XP Service Pack 3 (Important)	Windows XP Service Pack 3 (Important)
Windows XP Professional x64 Edition Service Pack 2	Windows XP Professional x64 Edition Service Pack 2 (Critical)	Windows XP Professional x64 Edition Service Pack 2 (Critical)	Windows XP Professional x64 Edition Service Pack 2 (Critical)	Windows XP Professional x64 Edition Service Pack 2 (Important)	Windows XP Professional x64 Edition Service Pack 2 (Important)	Windows XP Professional x64 Edition Service Pack 2 (Important)	Windows XP Professional x64 Edition Service Pack 2 (Important)	Windows XP Professional x64 Edition Service Pack 2 (Important)
Windows Server 2003								
Bulletin Identifier	**Bulletin 1**	**Bulletin 2**	**Bulletin 3**	**Bulletin 5**	**Bulletin 6**	**Bulletin 7**	**Bulletin 8**	**Bulletin 9**
Aggregate Severity Rating	Important	Critical	Critical	Important	Important	Important	Important	Important
Windows Server 2003 Service Pack 2	Windows Server 2003 Service Pack 2 (Important)	Windows Server 2003 Service Pack 2 (Critical)	Windows Server 2003 Service Pack 2 (Critical)	Windows Server 2003 Service Pack 2 (Important)	Windows Server 2003 Service Pack 2 (Important)	Windows Server 2003 Service Pack 2 (Important)	Windows Server 2003 Service Pack 2 (Important)	Windows Server 2003 Service Pack 2 (Important)
Windows Server 2003 x64 Edition Service Pack 2	Windows Server 2003 x64 Edition Service Pack 2 (Important)	Windows Server 2003 x64 Edition Service Pack 2 (Critical)	Windows Server 2003 x64 Edition Service Pack 2 (Critical)	Windows Server 2003 x64 Edition Service Pack 2 (Important)	Windows Server 2003 x64 Edition Service Pack 2 (Important)	Windows Server 2003 x64 Edition Service Pack 2 (Important)	Windows Server 2003 x64 Edition Service Pack 2 (Important)	Windows Server 2003 x64 Edition Service Pack 2 (Important)
Windows Server 2003 with SP2 for Itanium-based Systems	Windows Server 2003 with SP2 for Itanium-based Systems (Important)	Not applicable	Windows Server 2003 with SP2 for Itanium-based Systems (Critical)	Windows Server 2003 with SP2 for Itanium-based Systems (Important)	Windows Server 2003 with SP2 for Itanium-based Systems (Important)	Windows Server 2003 with SP2 for Itanium-based Systems (Important)	Windows Server 2003 with SP2 for Itanium-based Systems (Important)	Windows Server 2003 with SP2 for Itanium-based Systems (Important)

Windows Vista								
Bulletin Identifier	**Bulletin 1**	**Bulletin 2**	**Bulletin 3**	**Bulletin 5**	**Bulletin 6**	**Bulletin 7**	**Bulletin 8**	**Bulletin 9**
Aggregate Severity Rating	Important	Critical	Critical	Important	None	None	Important	None
Windows Vista Service Pack 1 and Windows Vista Service Pack 2	Windows Vista Service Pack 1 and Windows Vista Service Pack 2 (Important)	Windows Vista Service Pack 1 and Windows Vista Service Pack 2 (Critical)	Windows Vista Service Pack 1 and Windows Vista Service Pack 2 (Critical)	Windows Vista Service Pack 1 and Windows Vista Service Pack 2 (Important)	Not applicable	Not applicable	Windows Vista Service Pack 2 only (Important)	Not applicable
Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition Service Pack 2	Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition Service Pack 2 (Important)	Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition Service Pack 2 (Critical)	Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition Service Pack 2 (Critical)	Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition Service Pack 2 (Important)	Not applicable	Not applicable	Windows Vista x64 Edition Service Pack 2 only (Important)	Not applicable
Windows Server 2008								
Bulletin Identifier	**Bulletin 1**	**Bulletin 2**	**Bulletin 3**	**Bulletin 5**	**Bulletin 6**	**Bulletin 7**	**Bulletin 8**	**Bulletin 9**
Aggregate Severity Rating	Important	Critical	Critical	Important	None	None	Important	None
Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2	Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2* (Important)	Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2** (Critical)	Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2* (Critical)	Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2* (Important)	Not applicable	Not applicable	Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2* (Important)	Not applicable
Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2	Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2* (Important)	Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2** (Critical)	Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2* (Critical)	Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2* (Important)	Not applicable	Not applicable	Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2* (Important)	Not applicable

Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2	Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2 (Important)	Not applicable	Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2 (Critical)	Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2 (Important)	Not applicable	Not applicable	Not applicable	Not applicable
Windows 7								
Bulletin Identifier	**Bulletin 1**	**Bulletin 2**	**Bulletin 3**	**Bulletin 5**	**Bulletin 6**	**Bulletin 7**	**Bulletin 8**	**Bulletin 9**
Aggregate Severity Rating	**Important**	None	None	**Important**	None	None	**Important**	None
Windows 7 for 32-bit Systems	Windows 7 for 32-bit Systems (Important)	Not applicable	Not applicable	Windows 7 for 32-bit Systems (Important)	Not applicable	Not applicable	Windows 7 for 32-bit Systems (Important)	Not applicable
Windows 7 for x64-based Systems	Windows 7 for x64-based Systems (Important)	Not applicable	Not applicable	Windows 7 for x64-based Systems (Important)	Not applicable	Not applicable	Windows 7 for x64-based Systems (Important)	Not applicable
Windows Server 2008 R2								
Bulletin Identifier	**Bulletin 1**	**Bulletin 2**	**Bulletin 3**	**Bulletin 5**	**Bulletin 6**	**Bulletin 7**	**Bulletin 8**	**Bulletin 9**
Aggregate Severity Rating	**Important**	None	None	**Important**	None	None	**Important**	None
Windows Server 2008 R2 for x64-based Systems	Windows Server 2008 R2 for x64-based Systems* (Important)	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems* (Important)	Not applicable	Not applicable	Windows Server 2008 R2 for x64-based Systems* (Important)	Not applicable
Windows Server 2008 R2 for Itanium-based Systems	Windows Server 2008 R2 for Itanium-based Systems (Important)	Not applicable	Not applicable	Windows Server 2008 R2 for Itanium-based Systems (Important)	Not applicable	Not applicable	Not applicable	Not applicable

Notes for Windows Server 2008 and Windows Server 2008 R2

***Server Core installation affected.** This update applies, with the same severity rating, to supported editions of Windows Server 2008 or Windows Server 2008 R2 as indicated, whether or not installed using the Server Core installation option. For more information on this installation option, see the TechNet articles, Managing a Server Core Installation and Servicing a Server Core Installation. Note that the Server Core installation option does not apply to certain editions of Windows Server 2008 and Windows Server 2008 R2; see Compare Server Core Installation Options.

****Server Core installation not affected.** The vulnerabilities addressed by this update do not affect supported editions of Windows Server 2008 as indicated, when installed using the Server Core installation option. For more information on this installation option, see the TechNet articles, Managing a Server Core Installation and Servicing a Server Core Installation. Note that the Server Core installation option does not apply to certain editions of Windows Server 2008 and Windows Server 2008 R2; see Compare Server Core Installation Options.

Note for Bulletin 3

See also other software categories under this section, Affected Software and Download Locations, for more update files under the same bulletin identifier. This bulletin spans more than one software category.

Top of section

Microsoft Office Suites and Software

Microsoft Office Suites, Systems, and Components		
Bulletin Identifier	**Bulletin 3**	**Bulletin 4**
Aggregate Severity Rating	**Important**	**Critical**
Microsoft Office XP Service Pack 3	Microsoft Office XP Service Pack 3 (Important)	Microsoft Outlook 2002 Service Pack 3 (Critical)
Microsoft Office 2003 Service Pack 3	Microsoft Office 2003 Service Pack 3 (Important)	Microsoft Outlook 2003 Service Pack 3 (Important)
Microsoft Office 2007 Service Pack 2	Microsoft Office 2007 Service Pack 2 (Important)	Microsoft Outlook 2007 Service Pack 2 (Important)

Note for Bulletin 3

See also other software categories under this section, Affected Software and Download Locations, for more update files under the same bulletin identifier. This bulletin spans more than one software category.

Top of section

Top of section

Detection and Deployment Tools and Guidance

Security Central

Manage the software and security updates you need to deploy to the servers, desktop, and mobile computers in your organization. For more information see the TechNet Update Management Center. The TechNet Security Center provides additional information about security in Microsoft products. Consumers can visit Security At Home, where this information is also available by clicking "Latest Security Updates".

Security updates are available from Microsoft Update and Windows Update. Security updates are also available at the Microsoft Download Center. You can find them most easily by doing a keyword search for "security update".

Finally, security updates can be downloaded from the Microsoft Update Catalog. The Microsoft Update Catalog provides a searchable catalog of content made available through Windows Update and Microsoft Update, including security updates, drivers and service packs. By searching using the security bulletin number (such as, "MS07-036"), you can add all of the applicable updates to your basket (including different languages for an update), and download to the folder of your choosing. For more information about the Microsoft Update Catalog, see the Microsoft Update Catalog FAQ.

Detection and Deployment Guidance

Microsoft provides detection and deployment guidance for security updates. This guidance contains recommendations and information that can help IT professionals understand how to use various tools for detection and deployment of security updates. For more information, see Microsoft Knowledge Base Article 961747.

Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer (MBSA) allows administrators to scan local and remote systems for missing security updates as well as common security misconfigurations. For more information about MBSA, visit Microsoft Baseline Security Analyzer.

Windows Server Update Services

By using Windows Server Update Services (WSUS), administrators can quickly and reliably deploy the latest critical updates and security updates for Windows 2000 operating systems and later, Office XP and later, Exchange Server 2003, and SQL Server 2000 to Windows 2000 and later operating systems.

For more information about how to deploy this security update using Windows Server Update Services, visit Windows Server Update Services.

Systems Management Server

Microsoft Systems Management Server (SMS) delivers a highly-configurable enterprise solution for managing updates. By using SMS, administrators can identify Windows-based systems that require security updates and to perform controlled deployment of these updates throughout the enterprise with minimal disruption to end users. The next release of SMS, System Center Configuration Manager 2007, is now available; see also System Center Configuration Manager 2007. For more information about how administrators can use SMS 2003 to deploy security updates, see SMS 2003 Security Patch Management. SMS 2.0 users can also use the Security Update Inventory Tool (SUIT) to help deploy security updates. For information about SMS, visit Microsoft Systems Management Server.

Note SMS uses the Microsoft Baseline Security Analyzer to provide broad support for security bulletin update detection and deployment. Some software updates may not be detected by these tools. Administrators can use the inventory capabilities of SMS in these cases to target updates to specific systems. For more information about this procedure, see Deploying Software Updates Using the SMS Software Distribution Feature. Some security updates require administrative rights following a restart of the system. Administrators can use the Elevated Rights Deployment Tool (available in the SMS 2003 Administration Feature Pack and in the SMS 2.0 Administration Feature Pack) to install these updates.

Update Compatibility Evaluator and Application Compatibility Toolkit

Updates often write to the same files and registry settings required for your applications to run. This can trigger incompatibilities and increase the time it takes to deploy security updates. You can streamline testing and validating Windows updates against installed applications with the Update Compatibility Evaluator components included with Application Compatibility Toolkit.

The Application Compatibility Toolkit (ACT) contains the necessary tools and documentation to evaluate and mitigate application compatibility issues before deploying Microsoft Windows Vista, a Windows Update, a Microsoft Security Update, or a new version of Windows Internet Explorer in your environment.

Top of section

Other Information

Microsoft Windows Malicious Software Removal Tool

Microsoft will release an updated version of the Microsoft Windows Malicious Software Removal Tool on Windows Update, Microsoft Update, Windows Server Update Services, and the Download Center.

Top of section

Non-Security, High-Priority 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.

Top of section

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 Web sites provided by program partners, listed in Microsoft Active Protections Program (MAPP) Partners.

Top of section

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.

Top of section

Support

- The affected software listed have 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.
- Customers in the U.S. and Canada can receive technical support from Security Support or 1-866-PCSAFETY. There is no charge for support calls that are associated with security updates. For more information about available support options, see Microsoft Help and Support.
- International customers can receive support from their local Microsoft subsidiaries. There is no charge for support that is associated with security updates. For more information about how to contact Microsoft for support issues, visit International Help and Support.

Top of section

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.

Top of section

Top of page

Manage Your Profile

© 2010 Microsoft Corporation. All rights reserved. Contact Us | Terms of Use | Trademarks | Privacy Statement

Microsoft