



eSecurity Advisory
DECEMBER 2007 MICROSOFT SECURITY BULLETIN RELEASE

The purpose of this update is to provide you with a summary of Microsoft's December 2007 Security Bulletin releases.

NEW BULLETINS

Microsoft is releasing the following security bulletins for newly discovered vulnerabilities:

MAXIMUM SEVERITY	BULLETIN NUMBER	PRODUCTS AFFECTED	IMPACT
Important	MS07-063	Windows Vista	Remote Code Execution
Critical	MS07-064	Windows 2000, Windows XP, Windows Server 2003, and Windows Vista	Remote Code Execution
Important	MS07-065	Windows 2000 & Windows XP	Remote Code Execution
Important	MS07-066	Windows Vista	Elevation of Privilege
Important	MS07-067	Windows XP and Windows Server 2003	Local Elevation of Privilege
Critical	MS07-068	Windows Media Format Runtime 7.1, 9, 9.5, 11 & Windows Media Services 9.1	Remote Code Execution
Critical	MS07-069	Windows 2000, Windows XP, Windows Server 2003, and Windows Vista	Remote Code Execution

Microsoft Windows Malicious Software Removal Tool

Microsoft is releasing an updated version of the Microsoft Windows Malicious Software Removal Tool on Windows Server Update Services (WSUS), Windows Update (WU) and the Download Center. Note that this tool will NOT be distributed using Software Update Services (SUS). Information on the Microsoft Windows Malicious Software Removal Tool can be located here:

<http://go.microsoft.com/fwlink/?LinkId=40573>

High-Priority Non-Security Updates on Microsoft Update (MU), Windows Update (WU), Windows Server Update Services (WSUS)

Microsoft is also releasing High-Priority NON-SECURITY updates today on WU, MU, and WSUS. For complete details on non-security updates being released, please review the following KB Article:

<http://support.microsoft.com/?id=894199>

A summary for this new bulletin may be found at:

<http://www.microsoft.com/technet/security/bulletin/ms07-dec.mspx>.

TechNet Webcast:

Information about Microsoft's September Security Bulletin Release

Microsoft will be discussing today's bulletin during their regularly scheduled December 2007 TechNet Security Bulletin webcast. A replay will be available 24 hours after the live Webcast at the same URL.

This month, the webcast will be held Wednesday, December 12, 2007 at 11:00 AM Pacific Time.

<http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?culture=en-US&EventID=1032344696>

Agencies are advised to review the information in the bulletins, test and deploy the updates immediately in their environments, if applicable.

Technical Details

Microsoft Security Bulletin MS07-063	
Bulletin Title	Vulnerability in SMBv2 Could Allow Remote Code Execution (942624)
Executive Summary	This important security update resolves a privately reported vulnerability in Server Message Block Version 2 (SMBv2). The vulnerability could allow an attacker to tamper with data transferred via SMBv2, which could allow remote code execution in domain configurations communicating with SMBv2.
Maximum Severity Rating	Important
Impact of Vulnerability	Remote Code Execution
Detection	Microsoft Baseline Security Analyzer can detect whether your computer system requires this update.
Affected Software	Windows. For more information, see the Affected Software section of the bulletin.
Restart Requirement	The update will require a restart.
Removal Information	Windows Vista and Windows Vista x64 Edition: Use Add or Remove Programs tool in Control Panel or the wusa.exe utility.
Bulletins Replaced by This Update	None
Full Details	http://www.microsoft.com/technet/security/bulletin/ms07-063.msp

Microsoft Security Bulletin MS07-064	
Bulletin Title	Vulnerabilities in DirectX Could Allow Remote Code Execution (941568)
Executive Summary	This critical security update resolves two privately reported vulnerabilities in Microsoft DirectX. These vulnerabilities could allow code execution if a user opened a specially crafted file used for streaming media in DirectX. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete

eSecurity Advisory: DECEMBER 2007 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information

December 13, 2007

	control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	
Maximum Severity Rating	Critical	
Impact of Vulnerability	Remote Code Execution	
Detection	Microsoft Baseline Security Analyzer can detect whether your computer system requires this update.	
Affected Software	Windows, DirectX, DirectShow. For more information, see the Affected Software section of the bulletin.	
Restart Requirement	The update will not require a restart, except in certain situations.	
Bulletins Replaced by This Update	MS05-050	
Full Details	http://www.microsoft.com/technet/security/bulletin/ms07-064.msp	

Microsoft Security Bulletin MS07-065		
Bulletin Title	Vulnerability in Message Queuing Could Allow Remote Code Execution (937894)	
Executive Summary	This important security update resolves a privately reported vulnerability in Message Queuing Service (MSMQ) that could allow remote code execution in implementations on Microsoft Windows 2000 Server, or elevation of privilege in implementations on Microsoft Windows 2000 Professional and Windows XP. An attacker must have valid logon credentials to exploit this vulnerability. An attacker could then install programs; view, change, or delete data; or create new accounts.	
Maximum Severity Rating	Important	
Impact of Vulnerability	Remote Code Execution	
Detection	Microsoft Baseline Security Analyzer can detect whether your computer system requires this update.	
Affected Software	Windows. For more information, see the Affected Software section of the bulletin.	
Restart Requirement	The update will require a restart.	
Bulletins Replaced by This Update	MS05-017	
Full Details	http://www.microsoft.com/technet/security/bulletin/ms07-065.msp	

Microsoft Security Bulletin MS07-066	
Bulletin Title	Vulnerability in Windows Kernel Could Allow Elevation of Privilege (943078)

eSecurity Advisory: DECEMBER 2007 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information

December 13, 2007

Executive Summary	This important security update resolves a privately reported vulnerability in the Windows kernel. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.	
Maximum Severity Rating	Important	
Impact of Vulnerability	Elevation of Privilege	
Detection	Microsoft Baseline Security Analyzer can detect whether your computer system requires this update.	
Affected Software	Windows. For more information, see the Affected Software section of the bulletin.	
Restart Requirement	The update will require a restart.	
Bulletins Replaced by This Update	None	
Full Details	http://www.microsoft.com/technet/security/bulletin/ms07-066.msp	

Microsoft Security Bulletin MS07-067		
Bulletin Title	Vulnerability in Macrovision Driver Could Allow Local Elevation of Privilege (944653)	
Executive Summary	This important security update resolves one publicly disclosed vulnerability. A local elevation of privilege vulnerability exists in the way that the Macrovision driver incorrectly handles configuration parameters. An attacker who successfully exploited this vulnerability could take complete control of the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	
Maximum Severity Rating	Important	
Impact of Vulnerability	Local Elevation of Privilege	
Detection	Microsoft Baseline Security Analyzer can detect whether your computer system requires this update.	
Affected Software	Windows. For more information, see the Affected Software section of the bulletin.	
Restart Requirement	The update will require a restart.	
Bulletins Replaced by This Update	None	
Full Details	http://www.microsoft.com/technet/security/bulletin/ms07-067.msp	

Microsoft Security Bulletin MS07-068	
Bulletin Title	Vulnerability in Windows Media File Format Could Allow Remote Code Execution (941569 and 944275)

eSecurity Advisory: DECEMBER 2007 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information

December 13, 2007

Executive Summary	This critical security update resolves a privately reported vulnerability in Windows Media Format. This vulnerability could allow remote code execution if a user viewed a specially crafted file in Windows Media Format Runtime. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	
Maximum Severity Rating	Critical	
Impact of Vulnerability	Remote Code Execution	
Detection	Microsoft Baseline Security Analyzer can detect whether your computer system requires this update.	
Affected Software	Windows, Windows Media Format Runtime. For more information, see the Affected Software section of the bulletin.	
Restart Requirement	The update will not require a restart, except in certain situations.	
Bulletins Replaced by This Update	MS06-078	
Full Details	http://www.microsoft.com/technet/security/bulletin/ms07-068.msp	

Microsoft Security Bulletin MS07-069		
Bulletin Title	Cumulative Security Update for Internet Explorer (942615)	
Executive Summary	This critical security update resolves four privately reported vulnerabilities. The most serious security impact could allow remote code execution if a user viewed a specially crafted Web page using Internet Explorer. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	
Maximum Severity Rating	Critical	
Impact of Vulnerability	Remote Code Execution	
Detection	Microsoft Baseline Security Analyzer can detect whether your computer system requires this update.	
Affected Software	Windows, Internet Explorer. For more information, see the Affected Software section of the bulletin.	
Restart Requirement	The update will require a restart.	
Bulletins Replaced by This Update	MS07-057	
Full Details	http://www.microsoft.com/technet/security/bulletin/ms07-069.msp	

PLEASE VISIT <http://www.microsoft.com/technet/security>
FOR THE MOST CURRENT INFORMATION ON THESE ALERTS.