



Summary of Critical Patches – December 2007

Microsoft Security Bulletin - MS07-064

Vulnerabilities in DirectX

MS07-064 Vulnerabilities in DirectX Could Allow Remote Code Execution

Affected Software

DirectX 7.0 and DirectX 8.1

Microsoft Windows 2000 Service Pack 4

DirectX 9.0c

Microsoft Windows 2000 Service Pack 4

Windows XP Service Pack 2

Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2

Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2

Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2

Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems

DirectX 10.0

Windows Vista

Windows Vista x64 Edition

Vulnerability

CVE-2007-3901

A remote code execution vulnerability exists in the way DirectX handles SAMI files.

Vulnerability Information

This vulnerability could allow code execution if a user opened a specially created SAMI file. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system.

The vulnerability lies in Microsoft DirectShow, an integrated technology of DirectX, and does not perform sufficient parsing of the parameters of Synchronized Accessible Media Interchange (SAMI) file types. Microsoft DirectShow is used for streaming media on Microsoft Windows operating systems.

Exploitation of this vulnerability would require a user to open a specially crafted format file. However, since the vulnerability is in the streaming component of Microsoft Windows, attacks can be launched from a specially crafted Web site or any application that delivers Web content.

CVE-2007-3895

A remote code execution vulnerability exists in the way DirectX handles WAV and AVI format files.

Vulnerability Information

This vulnerability could allow code execution if a user visits a specially crafted Web site or opens an e-mail message with specially crafted content. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system.

Comment / Mitigation

- There are currently no known exploits for this vulnerability; however GovCertUK recommend timely patching with all publicly known vulnerabilities.
- 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.
- See <http://www.microsoft.com/technet/security/bulletin/MS07-064.msp> for Windows XP mitigation steps.

References:

- <http://www.microsoft.com/technet/security/bulletin/MS07-064.msp>
- <http://www.securityfocus.com/>
- <http://isc.sans.org/diary.html?storyid=3735&rss>

Microsoft Security Bulletin - MS07-068

Vulnerability in Windows Media File Format

MS07-068 Vulnerability in Windows Media File Format Could Allow Remote Code Execution

Affected Software

Windows Media Format Runtime 7.1

Microsoft Windows 2000 Service Pack 4

Windows Media Format Runtime 9

Windows 2000 Service Pack 4

Windows XP Service Pack 2

Windows Media Format Runtime 9.5

Windows XP Service Pack 2

Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2

Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2

Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2

Windows Media Format Runtime 9.5 x64 Edition

Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2

Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2

Windows Media Format Runtime 11

Windows XP Service Pack 2

Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2

Windows Vista

Windows Vista x64 Edition

Windows Media Services 9.1

Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2

Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2

Vulnerability

CVE-2007-0064

This critical security update resolves a privately reported vulnerability in Windows Media File Format. This vulnerability could allow remote code execution if a user viewed a specially crafted file in Windows Media Format Runtime.

Vulnerability Information

A remote code execution vulnerability exists in the Windows Media Format Runtime due to the way it handles Advanced Systems Format (ASF) files.

The Microsoft Windows Media Format Runtime provides information and tools for applications that use Windows Media content. ASF (Advanced Systems Format) is a file format that stores audio and video information and is specially designed to run over networks like the Internet.

In client applications, such as Windows Media Player, an attacker could exploit the vulnerability by constructing specially crafted Windows Media Format Runtime content that could potentially allow remote code execution if a user visits a specially crafted Web site or opens an e-mail message with specially crafted content.

In server applications, such as Windows Media Services, an attacker could exploit the vulnerability by constructing specially crafted Windows Media Format Runtime content that could potentially allow remote code execution if the server processes the specially crafted content.

In client and server applications, an attacker who successfully exploited this vulnerability could take complete control of an affected system.

Comment / Mitigation

This vulnerability requires that a user is logged on and opens the specially crafted ASF file in any Windows Media Format Runtime-based application for any malicious action to occur. Therefore systems where Windows Media Format Runtime or Windows Media Server 9.1 is used frequently, such as workstations or terminal servers, are most at risk from this vulnerability.

- There are currently no known exploits for this vulnerability; however GovCertUK recommend timely patching with all publicly known vulnerabilities.

References:

<http://www.microsoft.com/technet/security/bulletin/MS07-068.msp>
<http://www.securityfocus.com/>
<http://isc.sans.org/diary.html?storyid=3735&rss>

Microsoft Security Bulletin - MS07-069

Vulnerabilities in Internet Explorer

MS07-069 Vulnerabilities in Internet Explorer Could Allow Remote Code Execution

Affected Software

Internet Explorer 5.01 and Internet Explorer 6 Service Pack 1

Microsoft Windows 2000 Service Pack 4

Internet Explorer 6

Windows XP Service Pack 2

Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2

Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2

Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2

Internet Explorer 7

Windows XP Service Pack 2

Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2

Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2

Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2

Windows Vista

Windows Vista x64 Edition

Vulnerabilities

CVE-2007-3902, CVE-2007-3903, CVE-2007-5344

A remote code execution vulnerability exists in the way Internet Explorer accesses an object that has not been correctly initialised or that has been deleted.

Vulnerability Information

This vulnerability exists when Internet Explorer attempts to access an object which has not been initialised or has been deleted. As a result, memory may be corrupted in such a way that an attacker could execute arbitrary code in the context of the logged-on user.

An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

An attacker could host a specially crafted Web site that is designed to exploit these vulnerabilities through Internet Explorer and then convince a user to visit the Web site. This could also include compromised Web sites and Web sites that accept or host user-provided content or advertisements.

In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or in an Instant Messenger message that takes users to the attacker's Web site. It could also be possible to display specially crafted Web content by using banner advertisements or by using other methods to deliver Web content to affected systems.

CVE-2007-5347

A remote code execution vulnerability exists in the way Internet Explorer displays a Web page that contains certain unexpected method calls to HTML objects. As a result, system memory may be corrupted in such a way that an attacker could execute arbitrary code if a user visited a specially crafted Web site. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

An attacker could host a specially crafted Web site that is designed to exploit this vulnerability through Internet Explorer and then convince a user to view the Web site. This can also include compromised Web sites and Web sites that accept or host user-provided content or advertisements. These Web sites 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 these Web sites.

Comment / Mitigation

- This vulnerability is being actively exploited and GovCertUK recommended immediate patching.
- An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. 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.

References:

<http://www.microsoft.com/technet/security/bulletin/MS07-069.mspx>
<http://www.securityfocus.com/>
<http://isc.sans.org/diary.html?storyid=3735&rss>

Summary of Important Patches

Microsoft Security Bulletin - MS07-063

Vulnerability in SMBv2

MS07-063 Vulnerability in SMBv2 Could Allow Remote Code Execution

Affected Software

Windows Vista
Windows Vista x64

Vulnerability

A remote code execution vulnerability exists in the SMBv2 protocol that could allow a remote anonymous attacker to run code with the privileges of the logged-on user.

Vulnerability Information

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.

Server Message Block (SMB) is the file sharing protocol used by default on Windows based computers. SMB Version 2.0 (SMBv2) is an update to this protocol and is only supported on computers running Windows Server 2008 and Windows Vista. SMBv2 can only be used if both client and server support it. The SMB protocol version to be used for file operations is decided during the negotiation phase. During the negotiation phase, a Windows Vista client advertises to the server that it can understand the new SMBv2 protocol. If the server (Windows Server 2008 or otherwise) understands SMBv2, then SMBv2 is chosen for subsequent communication. Otherwise the client and server use SMB 1.0.

SMBv2 signing is a feature through which all communications using the Server Message Block (SMB) protocol can be digitally signed at the packet level. Digitally signing the packets enables the recipient of the packets to confirm their point of origin and their authenticity.

This security update addresses the vulnerability by implementing proper signing using SMBv2.

Comment / Mitigation:

- SMB signing is off by default in Windows Vista, which means that a computer running Microsoft Vista won't use it unless it connects to another host which requires it.
- When a previous operating system version is part of the communications, SMBv2 will not be used. For example, Windows Vista would use SMB to communicate with Windows XP, rather than SMBv2.
- Customers using SMBv1 are not affected by this vulnerability.

- Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

References:

<http://www.microsoft.com/technet/security/bulletin/ms07-063.msp>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5351>

Microsoft Security Bulletin - MS07-065

Vulnerability in Message Queuing

MS07-065 Vulnerability in Message Queuing Could Allow Remote Code Execution

Affected Software

Microsoft Windows 2000 Server Service Pack 4 (Remote Code Execution Possible)

Microsoft Windows 2000 Professional Service Pack 4 (Remote Code Execution Possible)

Windows XP Service Pack 2 (Elevation of Privilege)

Vulnerability

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.

Vulnerability Information

Microsoft Message Queuing technology enables applications that are running at different times to communicate across heterogeneous networks and across systems that may be temporarily offline. Applications send messages to queues and read messages from queues. Message Queuing provides guaranteed message delivery, efficient routing, security, and priority-based messaging. It can be used to implement solutions for both asynchronous and synchronous messaging scenarios. For more information about Message Queuing, see the Message Queuing product documentation

A remote code execution vulnerability exists in the Message Queuing Service when it incorrectly validates input strings before passing the strings to a buffer. An attacker could exploit the vulnerability by constructing a specially crafted MSMQ message. This could allow remote code execution in a remote attack scenario on Microsoft Windows 2000 Server and a local elevation of privilege in a local scenario on Microsoft Windows 2000 Professional and Windows XP. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

The update removes the vulnerability by modifying the way that the MSMQ service validates input strings before passing the strings to the allocated buffer.

Comment / Mitigation:

- An attacker must have valid logon credentials in order to exploit this vulnerability on Microsoft 2000 Professional and Windows XP.
- By default, the Message Queuing component is not installed on any affected operating system edition and can only be enabled by a user with administrative privileges. Only customers who manually install the Message Queuing component are likely to be vulnerable.
- For customers that require the Message Queuing component, firewall best practices and default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed
- Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

References:

<http://www.microsoft.com/technet/security/bulletin/ms07-065.msp>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3039>

Microsoft Security Bulletin - MS07-066

Vulnerability in Windows Kernel

MS07-066 Vulnerability in Windows kernel Could Allow Elevation of Privilege

Affected Software

Windows Vista
Windows Vista x64

Vulnerability

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.

Vulnerability Information

The kernel is the core of the operating system and it provides basic services for all other parts of the operating system.

An elevation of privilege vulnerability exists in the way that the Windows kernel processes certain access requests. This vulnerability could allow an attacker to run code and to take complete control of the system. 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.

Microsoft Monthly Patch Summary - Date: 11th December 2007

The update removes the vulnerability by modifying the way that the Windows kernel validates certain conditions in legacy reply paths.

Comment / Mitigation:

- An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. The vulnerability can not be exploited remotely or by anonymous users.
- At the time of posting Microsoft has not received any information to indicate that this vulnerability has been publicly used to attack customers and has not seen any examples of proof of concept code published.

References:

<http://www.microsoft.com/technet/security/bulletin/MS07-066.aspx>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5350>

Microsoft Security Bulletin - MS07-067

Vulnerability in Macrovision Driver

MS07-067 Vulnerability in Macrovision Driver Could Allow Local Elevation of Privilege

Affected Software

Windows XP Service Pack 2
Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2
Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2

Vulnerability

A local elevation of privilege vulnerability exists in the way that the Macrovision driver incorrectly handles configuration parameters.

Vulnerability Information

An attacker who successfully exploited this vulnerability could execute arbitrary code in the context of the local system. An attacker could then install programs, view, change, or delete data or create new accounts with full administrative rights.

The driver, `secdrv.sys`, is used by games which use Macrovision SafeDisc. The driver validates the authenticity of games that are protected with SafeDisc and prohibits unauthorised copies of such games to play on Windows. The `secdrv.sys` is included with Microsoft Windows XP, Windows Server 2003, and Windows Vista to increase compatibility of the games on Windows. Without the driver, games with SafeDisc protection would be unable to play on Windows. SafeDisc remains inactive until invoked by a game for authorisation to play on Windows.

Comment / Mitigation:

- An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. The vulnerability could not be exploited remotely or by anonymous users.
- An attacker must convince a user to run an executable or must have valid logon credentials to exploit this vulnerability. This is a local elevation of privilege vulnerability. The exploit for this vulnerability can not be done remotely.
- This vulnerability is being actively exploited and is therefore classed as "Critical" by a number of security communities.

References:

<http://www.microsoft.com/technet/security/bulletin/MS07-067.msp>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5350>