



Summary of Critical Patches – June 2008

Microsoft Security Bulletin - MS08-030

Vulnerability in Bluetooth Stack

MS08-030 Vulnerability in Bluetooth Stack could allow Remote Code Execution

Vulnerability Details

A remote code execution vulnerability exists in the Windows Bluetooth stack. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

This security update addresses the vulnerability by modifying the way that the Bluetooth stack handles a large number of service description requests.

Affected Software

Windows XP Service Pack 2 and Windows XP Service Pack 3

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

Windows Vista and Windows Vista Service Pack 1

Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1

Vulnerability Details

Bluetooth Vulnerability - CVE-2008-1453

The vulnerability exists as the Windows Bluetooth Stack does not correctly handle a large number of service description requests. To exploit this vulnerability an attacker would have to send a flood of specifically crafted SDP packets to an affected system. The attacker could then take complete control of an affected system.

Comment / Mitigation

Microsoft have not identified mitigation advice other than applying the patch, however they do emphasise that this vulnerability only affects systems with Bluetooth capability. Bluetooth devices and built in Bluetooth chips in laptops etc. can be switched off to prevent exploitation.

References:

<http://www.microsoft.com/technet/security/bulletin/MS08-030.mspx>

Microsoft Security Bulletin - MS08-031

Update for Internet Explorer

MS08-031 Cumulative Security Update for Internet Explorer

Vulnerability Details

This security update resolves one privately reported and one publicly disclosed vulnerability. The privately reported vulnerability could allow remote code execution if a user viewed a specially crafted Web page using Internet Explorer. The publicly disclosed vulnerability could allow information disclosure if a user viewed a specially crafted Web page using Internet Explorer.

The security update addresses these vulnerabilities by modifying the way that Internet Explorer handles calls to HTML objects and validates data.

Affected Software

- Internet Explorer 5.01 and Internet Explorer 6 Service Pack 1 running on:
 - Microsoft Windows 2000 Service Pack 4
 - Microsoft Windows 2000 Service Pack 4
- Internet Explorer 6 running on:
 - Windows XP Service Pack 2 and Windows XP Service Pack 3
 - 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
- Internet Explorer 7 running on:
 - Windows XP Service Pack 2 and Windows XP Service Pack 3
 - 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
 - Windows Vista and Windows Vista Service Pack 1
 - Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1
 - Windows Server 2008 for 32-bit Systems*
 - Windows Server 2008 for x64-based Systems*
 - Windows Server 2008 for Itanium-based Systems

Vulnerability Details

HTML Objects Memory Corruption Vulnerability –

CVE-2008-1442 A remote code execution vulnerability exists in the way Internet Explorer displays a Web page that contains certain unexpected method calls to HTML objects. 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 this vulnerability through Internet Explorer and then convince a user to view the Web site. This could 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.

Request Header Cross-Domain Information Disclosure Vulnerability – CVE-2008-1544

An information disclosure vulnerability exists in the way Internet Explorer handles certain header requests. This vulnerability is caused by Internet Explorer incorrectly parsing specially crafted header requests, allowing a violation of the same origin policy.

An attacker who successfully exploited this vulnerability could read data from another domain in Internet Explorer.

Comment / Mitigation

Mitigation factors – Set 1 applies.

References:

<http://www.microsoft.com/technet/security/bulletin/MS08-031.msp>

Microsoft Security Bulletin - MS08-033

Vulnerabilities in DirectX

MS08-033 Vulnerabilities in DirectX Could Allow Remote Code Execution

Vulnerability Details

This security update resolves two privately reported vulnerabilities in Microsoft DirectX that could allow remote code execution if a user opens a specially crafted media file. An attacker who successfully exploited either of these vulnerabilities could take complete control of an affected system.

This is a critical security update for all supported editions of Microsoft Windows 2000, Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008.

This security update addresses the vulnerability by modifying the way that DirectX handles MJPEG and SAMI format files.

Affected Software

DirectX 7.0 and DirectX 8.1
Microsoft Windows 2000 Service Pack 4
Microsoft Windows 2000 Service Pack 4
DirectX 9.0*
Microsoft Windows 2000 Service Pack 4
Windows XP Service Pack 2 and Windows XP Service Pack 3
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 with Service Pack 1
Windows Vista x64 Edition
Windows Vista x64 Edition with Service Pack 1
Windows Server 2008 for 32-bit Systems*
Windows Server 2008 for x64-based Systems*
Windows Server 2008 for Itanium-based Systems

Vulnerability Details

MJPEG Decoder Vulnerability - CVE-2008-0011

An MJPEG is a media file where a number of JPEG images are connected together to create a video stream. The MJPEG video stream can then be inserted into an AVI or other common video formatted file. Audio Video Interleave (AVI) and Advanced Systems Format (ASF) files are two types of multimedia files commonly used by Windows Media Player.

A remote code execution vulnerability exists in the way the Windows MJPEG Codec handles MJPEG streams in AVI or ASF files. A user would have to preview or play a specially crafted MJPEG file for the vulnerability to be exploited.

Exploitation of the vulnerability would require a user to open and view a media file with a specially crafted MJPEG file embedded in it.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a media file with a specially crafted MJPEG file embedded in it to the user and by convincing the user to open the file.

In a Web-based attack scenario, an attacker would have to host a Web site that contains specially crafted content that is used to attempt to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content could contain specially crafted content that could exploit this vulnerability.

SAMI Format Parsing Vulnerability - CVE-2008-1444

A remote code execution vulnerability exists in the way DirectX handles supported format files. This vulnerability could allow remote code execution if a user opened a specially crafted file.

This vulnerability exists as DirectX does not perform sufficient parsing of the parameters of Synchronized Accessible Media Interchange (SAMI) file types.

SAMI (Microsoft Synchronized Accessible Media Interchange) was designed and developed to caption the digital media widely available in PC systems. SAMI captions coexist with digital media as separate, simple text files. The captions can be easily modified, maintained, customized, and localized for different languages.

Comment / Mitigation

Mitigation factors – Set 1 apply

References:

<http://www.microsoft.com/technet/security/bulletin/MS08-033.msp>

Summary of Important Patches

Microsoft Security Bulletin - MS08-034

Vulnerability in WINS

MS08-034 Vulnerability in WINS could allow Elevation of Privilege

This security update resolves a privately reported vulnerability. A local attacker who successfully exploited this vulnerability could take complete control of an affected system.

Affected Software

Microsoft Windows 2000 Server Service Pack 4
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

Vulnerability Details

Memory Overwrite Vulnerability - CVE-2008-1451

An elevation of Privilege vulnerability exists in WINS because it does not correctly validate the data structures within specifically crafted WINS network packets. The vulnerability could allow an attacker to run code with elevated privileges. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

To exploit this vulnerability an attacker would have to send a specifically crafted network packet to the affected WINS server.

Cause of vulnerability

WINS does not correctly validate the data structures within specifically crafted WINS network packets.

What is WINS?

Although NetBIOS and NetBIOS names can be used with network protocols other than TCP/IP, Windows Internet Naming Service (WINS) was designed specifically to support NetBIOS over TCP/IP (NetBT). WINS is required for any environment in which users access resources that have NetBIOS names.

Comment / Mitigation

No mitigation advice has been identified by Microsoft. As a workaround their recommendation is to block UDP ports 1024 – 5000 (these are the random port ranges that WINS uses) at the perimeter firewall.

These ports are used to initiate a connection with a remote WINS server. If you block these ports at the perimeter firewall, you help prevent computers that are behind that firewall from trying to use this vulnerability. We recommend blocking all incoming unsolicited communication from the Internet.

References:

<http://www.microsoft.com/technet/security/bulletin/MS08-034.msp>

Microsoft Security Bulletin - MS08-035

Vulnerability in Active Directory Service

MS08-035 Vulnerability in Active Directory Could Allow Denial of Service

This security update resolves a privately reported vulnerability in implementations of Active Directory on Microsoft Windows 2000 Server, Windows Server 2003 and Windows Server 2008, Active Directory Application Mode (ADAM) when installed on Windows XP and Windows Server 2003, and Active Directory Lightweight Directory Service (AD LDS) when installed on Windows Server 2008. The vulnerability could allow a denial of service condition.

This security update addresses the vulnerability by validating client LDAP requests.

Affected Software

Microsoft Windows 2000 Server Service Pack 4
Windows XP Professional Service Pack 2
Windows XP Professional Service Pack 3
Windows XP Professional x64 Edition and Windows XP Professional Edition Service Pack 2
Windows Server 2003 Service Pack 1 and Windows Server 2003 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 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
Windows Server 2008 for 32-bit Systems*
Windows Server 2008 for 32-bit Systems*
Windows Server 2008 for x64-based Systems*
Windows Server 2008 for x64-based Systems*

Vulnerability Details

Active Directory Vulnerability - CVE-2008-1445

The vulnerability is due to improper validation of specially crafted LDAP requests. An attacker who successfully exploited this vulnerability could cause the computer to stop responding and automatically restart. Note that the denial of service vulnerability would not allow an attacker to execute code or to elevate their user rights, but it could cause the affected system to stop accepting requests.

ADAM is a Lightweight Directory Access Protocol (LDAP) directory service that runs as a user service for Windows XP and Windows Server 2003, rather than as a system service.

AD LDS is a Lightweight Directory Access Protocol (LDAP) directory service that runs as a user service for Windows Server 2008, rather than as a system service.

An attacker could try to exploit the vulnerability by sending a specially crafted LDAP packet to the ADAM or an Active Directory server. For Windows 2000 Server, any anonymous user with access to the target network could deliver a specially crafted network packet to the affected system in order to exploit this vulnerability. On Windows Server 2003 or systems with ADAM installed, the attacker must have valid authentication credentials in order to exploit this vulnerability.

Comment / Mitigation

Microsoft has not identified any mitigating factors for this vulnerability.

References: <http://www.microsoft.com/technet/security/bulletin/MS08-035.mspx>

Microsoft Security Bulletin - MS08-036

Vulnerabilities in Pragmatic General Multicast (PGM)

MS08-036 Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service

This security update resolves two privately reported vulnerabilities in the Pragmatic General Multicast (PGM) protocol that could allow a denial of service if malformed PGM packets are received by an affected system. An attacker who successfully exploited this vulnerability could cause a user's system to become non-responsive and may require a reboot to restore functionality.

Note that the denial of service vulnerability would not allow an attacker to execute code or to elevate their user rights, but it could cause the affected system to stop accepting requests.

This is an important security update for all supported editions of Windows XP and Windows Server 2003 and a moderate security update for all supported editions of Windows Vista and Windows Server 2008.

Affected Software

Affected Software	PGM Invalid Length Vulnerability - CVE-2008-1440	PGM Malformed Fragment Vulnerability - CVE-2008-1441	Aggregate Severity Rating
Windows XP Service Pack 2	Important Denial of Service	Moderate Denial of Service	Important
Windows XP Service Pack 3	Important Denial of Service	Moderate Denial of Service	Important
Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2	Important Denial of Service	Moderate Denial of Service	Important
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2	Important Denial of Service	Moderate Denial of Service	Important
Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service	Important Denial of Service	Moderate Denial of Service	Important

Microsoft Monthly Patch Summary - Date: 10th June 2008

Pack 2			
Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems	Important Denial of Service	Moderate Denial of Service	Important
Windows Vista and Windows Vista Service Pack 1	Not affected	Moderate Denial of Service	Moderate
Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1	Not affected	Moderate Denial of Service	Moderate
Windows Server 2008 for 32-bit Systems*	Not affected	Moderate Denial of Service	Moderate
Windows Server 2008 for x64-based Systems*	Not affected	Moderate Denial of Service	Moderate
Windows Server 2008 for Itanium-based Systems	Not affected	Moderate Denial of Service	Moderate

Vulnerability Details

PGM Invalid Length Vulnerability - CVE-2008-1440

A denial of service vulnerability exists in implementations of the Pragmatic General Multicast (PGM) protocol on Microsoft Windows XP and Windows Server 2003. The vulnerability is due to improper validation of specially crafted PGM packets.

PGM is a reliable and scalable multicast protocol that enables receivers to detect loss, request retransmission of lost data, or notify an application of unrecoverable loss. PGM is a receiver-reliable protocol, which means the receiver is responsible for ensuring all data is received, absolving the sender of reception responsibility.

An attacker could try to exploit the vulnerability by sending a specially crafted PGM packet to an affected system. The packet could then cause the affected system to become non-responsive until restarted.

PGM Malformed Fragment Vulnerability - CVE-2008-1441

A denial of service vulnerability exists in implementations of the Pragmatic General Multicast (PGM) protocol on Microsoft Windows XP, Windows Server 2003, Windows Vista, and Windows

Microsoft Monthly Patch Summary - Date: 10th June 2008

Server 2008. The protocol's parsing code does not properly validate specially crafted PGM fragments and will cause the affected system to become non-responsive until the attack has ceased.

The vulnerability is caused by the protocol's parsing code not properly handling malformed PGM packets that contain an invalid fragment option.

Comment / Mitigation

- On systems running Windows XP or Windows Server 2003, Pragmatic General Multicast (PGM) is only enabled when Microsoft Message Queuing (MSMQ) 3.0 is installed. The MSMQ service is not installed by default.
- On systems running Windows Vista or Windows Server 2008, Pragmatic General Multicast (PGM) is only enabled when Microsoft Message Queuing (MSMQ) 4.0 is installed and PGM is specifically enabled. The MSMQ service is not installed by default. When the MSMQ service is installed, the PGM protocol is available but not enabled by default.

References:

<http://www.microsoft.com/technet/security/bulletin/MS08-036.mspx>

Summary of Moderate Patches

Microsoft Security Bulletin - MS08-032

MS08-032- Cumulative Security Update of ActiveX Kill Bits

This security update resolves a publicly reported vulnerability for the Microsoft Speech API. The vulnerability could allow remote code execution if a user viewed a specially crafted Web page using Internet Explorer and has the Speech Recognition feature in Windows enabled.

The security update addresses the vulnerability by setting a kill bit so the vulnerable controls do not run in Internet Explorer.

Affected Software

Microsoft Windows 2000 Service Pack 4

Windows XP Service Pack 2

Windows XP Service Pack 3

Windows XP Professional x64 Edition and Windows XP Professional x64 Edition

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

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

2003 with SP2 for Itanium-based Systems

Windows Vista and Windows Vista Service Pack 1

Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1

Windows Server 2008 for 32-bit Systems*

Windows Server 2008 for x64-based Systems*

Windows Server 2008 for Itanium-based Systems

Vulnerability Details

The Speech API Vulnerability - CVE-2007-0675

A remote code execution vulnerability exists in the Speech Components sapi.dll. 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. The user must have the Speech Recognition feature in Windows enabled. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

This control was never intended to be instantiated in Internet Explorer.

Comment / Mitigation

- By default the speech recognition feature of Windows Vista is not enabled.
- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content could contain specially crafted content that could exploit this vulnerability.

References:

<http://www.microsoft.com/technet/security/bulletin/MS08-036.msp>

Mitigation information and factors

Mitigation Information and factors

Mitigation refers to a software setting, common configuration or general best practice, existing in a default state that could reduce the severity of exploitation of vulnerability. The following mitigating factors may be helpful for securing your systems.

Mitigation factors – Set 1

In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content could contain specially crafted content that could exploit this vulnerability. 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 or Instant Messenger message that takes users to the attacker's Web site.

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.

Mitigation factors – Set 2

The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful, a user must open an attachment that is sent in an e-mail message.