



Microsoft Monthly Patch Summary

Date: 12th June 2007

Summary of Critical Patches

Microsoft Security Bulletin - MS07-031

Vulnerability in Windows Schannel Security Package

MS07-031 Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution

Affected Software

Windows 2000 Service Pack 4
Windows XP Service Pack 2
Windows XP x64 and Windows XP x64 Service Pack 2
Windows Server 2003 Service Pack 1 and Service Pack 2
Windows Server 2003 x64 and Windows Server 2003 x64 Service Pack 2
Windows Server 2003 SP1 for Itanium-based Systems and SP2 for Itanium-based Systems

Vulnerability

This update resolves a privately reported vulnerability in the Secure Channel (Schannel) security package in Windows.

The Schannel security package implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Internet standard authentication protocols. This vulnerability could allow remote code execution if a user viewed a specially crafted Web page using a browser or an application that makes use of SSL/TLS. However, attempts to exploit this vulnerability would most likely result in the browser or application exiting. The system would not be able to connect to Web sites or resources using SSL or TLS until a restart of the system.

CVE-2007-2218

This vulnerability is caused by an off-by-one overflow error in the "ReverseMemCopy()" and "Ssl3ParseServerKeyExchange()" function within the Secure Channel (Schannel) module when handling a specially crafted digital signature during the SSL handshake, which could be exploited by remote attackers to execute arbitrary code by tricking a user into visiting a malicious web site.

Comment:

There is proof of concept exploit code available and Microsoft advise that there is no known workaround for this vulnerability.

GovCertUK advises timely patching as this vulnerability is in the public domain.

Microsoft Monthly Patch Summary - Date: 12th June 2007

References:

<http://www.microsoft.com/technet/security/Bulletin/MS07-031.msp>
<http://www.frsirt.com/english/advisories/2007/2151>

Microsoft Security Bulletin - MS07-033

Vulnerabilities in Internet Explorer

MS07-033 Cumulative Security Update for Internet Explorer

Affected Software

Internet Explorer 5.01, 6, 7

Vulnerabilities

This update resolves five privately reported vulnerabilities and one publicly disclosed vulnerability. All but one of these vulnerabilities could allow remote code execution if a user viewed a specially crafted Web page using Internet Explorer. One vulnerability could allow spoofing, and also involves a specially crafted Web page. In all remote code execution cases, 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. For the spoofing case, exploitation requires user interaction. This security update addresses two vulnerabilities by setting the kill bit for COM objects and for the rest, by modifying the way that Internet Explorer handles calls, error conditions, and special features such as Language Pack Installation and Speech Control. This security update replaces MS07-027,

CVE-2007-0218

A remote code execution vulnerability exists in the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer, causing a memory corruption error. An attacker could exploit this 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 take complete control of an affected system.

CVE-2007-1750

A remote code execution vulnerability exists in Internet Explorer due to improper handling of a CSS tag, causing a memory corruption error. 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 take complete control of an affected system.

CVE-2007-3027

A remote code execution vulnerability exists in Internet Explorer in the way that it handles multiple language pack installation, causing a race condition. 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 take complete control of an affected system. User interaction, while expected, is required to exploit this vulnerability.

CVE-2007-1751

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, causing a memory corruption error. 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 take complete control of an affected system.

CVE-2007-1499

A spoofing vulnerability exists in Internet Explorer that could allow an attacker to display spoofed content in the Navigation cancelled page. 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 take complete control of an affected system.

CVE-2007-2222

A remote code execution vulnerability exists in a component of Microsoft Speech API 4. 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 take complete control of an affected system.

Comment:

An attacker who successfully exploited these vulnerabilities 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.

Microsoft had not received any information to indicate that these vulnerabilities had been publicly used to attack customers, and had not seen any examples of public domain proof of concept code published when this security bulletin was issued.

GovCertUK advises timely patching as these vulnerabilities are likely to be exploited in the near future.

References:

<http://www.microsoft.com/technet/security/bulletin/ms07-033.mspx>
<http://www.frsirt.com/english/advisories/2007/2153>

Microsoft Security Bulletin - MS07-034

Vulnerabilities in Outlook Express and Windows Mail

MS07-034 Cumulative Security Update for Outlook Express and Windows Mail

Affected Software

Microsoft Outlook Express 6
Microsoft Windows Mail
Microsoft Windows XP Service Pack 2
Microsoft Windows XP Professional x64 Edition
Microsoft Windows XP Professional x64 Edition Service Pack 2
Microsoft Windows Server 2003 Service Pack 1
Microsoft Windows Server 2003 Service Pack 2
Microsoft Windows Server 2003 x64 Edition
Microsoft Windows Server 2003 x64 Edition Service Pack 2
Microsoft Windows Server 2003 SP1 (Itanium)
Microsoft Windows Server 2003 SP2 (Itanium)
Microsoft Windows Vista
Microsoft Windows Vista x64 Edition

Vulnerabilities

This critical security update resolves two privately reported and two publicly disclosed vulnerabilities.

A number of vulnerabilities have been identified in Microsoft Outlook Express and Windows Mail, which could be exploited by remote attackers to disclose sensitive information or take complete control of an affected system.

One of these vulnerabilities could allow remote code execution if a user viewed a specially crafted e-mail using Windows Mail in Windows Vista.

The other vulnerabilities may allow information disclosure if a user visits a specially crafted Web page using Internet Explorer and cannot be exploited directly in Outlook Express.

CVE-2007-2111

URL Redirect Cross Domain Information Disclosure Vulnerability

An information disclosure vulnerability exists in Windows because the MHTML protocol handler incorrectly interprets the MHTML URL redirections that could potentially bypass Internet Explorer domain restrictions. An attacker could exploit this with a malicious web site to bypass domain restrictions and read data from another domain.

CVE-2007-1658

Windows Mail UNC Navigation Request Remote Code Execution Vulnerability

This vulnerability is caused by a memory corruption error when handling specially crafted local or UNC navigation requests, which could be exploited by attackers to execute arbitrary code by tricking a user into clicking a specially crafted link in an e-mail message when using Windows Mail in Microsoft Windows Vista

CVE-2007-2225

URL Parsing Cross Domain Information Disclosure Vulnerability

An information disclosure vulnerability exists in Windows because the MHTML protocol handler incorrectly interprets HTTP headers when returning MHTML content. An attacker could exploit the vulnerability by constructing a specially crafted Web page. If the user viewed the Web page using Internet Explorer, the vulnerability could potentially allow information disclosure. An attacker who successfully exploited this vulnerability could read data from another Internet Explorer domain.

CVE-2007-2227

Content Disposition Parsing Cross Domain Information Disclosure Vulnerability

An information disclosure vulnerability exists in the way MHTML protocol handler passes Content-Disposition notifications back to Internet Explorer. The vulnerability could allow an attacker to bypass the file download dialogue box in Internet Explorer. An attacker could exploit the vulnerability by constructing a specially crafted Web page. If the user viewed the Web page using Internet Explorer, the vulnerability could potentially allow information disclosure. An attacker who successfully exploited this vulnerability could read data from another Internet Explorer domain.

Comment

There is very little technical information with regards to these vulnerabilities, and no exploit code was known to be in the public domain when this vulnerability was disclosed.

GovCertUK advises timely patching as these vulnerabilities are likely to be exploited in the near future.

References:

<http://www.frsirt.com/english/advisories/2007/1710>

<http://www.microsoft.com/technet/security/bulletin/ms07-025.mspx>

<http://www.auscert.org.au/render.html?it=7561>

Microsoft Security Bulletin - MS07-035

Vulnerability in Win 32 API

MS07-035 Vulnerability in Win 32 API Could Allow Remote Code Execution

Affected Software

Windows 2000 Service Pack 4

Windows XP Service Pack 2

Windows XP x64 and Windows XP x64 Service Pack 2

Windows Server 2003 Service Pack 1 and Service Pack 2

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

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

Vulnerabilities

CVE-2007-2219

A remote code execution vulnerability exists in the way that the Win32 API validates parameters passed to certain functions. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user viewed the Web page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Comment

Microsoft had not received any information to indicate that these vulnerabilities had been publicly used to attack customers, and had not seen any examples of public domain proof of concept code published when this security bulletin was issued.

GovCertUK advises timely patching as these vulnerabilities are likely to be exploited in the near future.

References:

<http://www.microsoft.com/technet/security/Bulletin/ms07-035.msp>

<http://www.fsirt.com/english/advisories/2007/2155>

Summary of Important Patches

Microsoft Security Bulletin - MS07-030

Vulnerabilities in Microsoft Visio

MS07-030 Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution

Affected Software

Microsoft Visio 2002 Service Pack 2
Microsoft Visio 2003 Service Pack 2

Vulnerabilities

CVE-2007-0934
CVE-2007-0936

Two remote code execution vulnerabilities exist in Visio which could be exploited by remote attackers to gain complete control of an affected system.

The first is caused by Visio not handling crafted version numbers properly when processing the contents of a file.

The second is due to the way Visio handles the parsing of packed objects within the Visio file format.

Comment

An attacker would exploit these vulnerabilities by enticing a user into opening a malicious file, either on a website or as an attachment to an email. There are currently no known exploits for these vulnerabilities, and Visio Viewer 2003 and 2007 are not affected by these issues.

GovCertUK advises timely patching as these vulnerabilities are likely to be exploited in the near future.

References:

<http://www.microsoft.com/technet/security/Bulletin/MS07-030.mspx>
<http://www.frsirt.com/english/advisories/2007/2150>
<http://isc.sans.org/diary.html>

Summary of Moderate Patches

Microsoft Security Bulletin - MS07-032

Vulnerability in Windows Vista

MS07-032 Vulnerability in Windows Vista Could allow Information Disclosure

Affected Software

Windows Vista
Windows Vista x64 Edition

Vulnerability

CVE-2007-2229

An information disclosure vulnerability in Windows Vista could allow non-privileged users to access local user information data stores contained within the registry and the local files system. This could allow a local attacker to access account data and could lead to privilege escalation and full access to the affected system.

Comment

The vulnerability is caused by incorrect permission settings that are set by default to a level that may allow low-privileged users access to administrative (and other) passwords.

Microsoft state that this vulnerability is not exploitable over the internet. An attacker would require local access, and currently there are no known exploits for this vulnerability.

GovCertUK advises timely patching as these vulnerability is likely to be exploited in the near future.

References:

<http://www.microsoft.com/technet/security/bulletin/ms07-032.mspx>
<http://www.frsirt.com/english/advisories/2007/2152>
<http://isc.sans.org/diary.html>