



Summary of Critical Patches

Patch Details - MS07-018

Vulnerabilities in MS Content Management Server – 11th April 2007

MS07-018 Vulnerabilities in MS Content Management Server Could Allow Remote Code Execution

Affected Software

Microsoft Content Management Server 2001 Service Pack 1
Microsoft Content Management Server 2002 Service Pack 2

Vulnerabilities:

Two vulnerabilities have been identified in Microsoft Content Management Server, which could be exploited by remote attackers to execute arbitrary code.

The first issue is caused by a memory corruption error when processing unexpected characters in an HTTP request, which could be exploited by attackers to remotely take complete control of an affected system.

The second vulnerability is caused by an input validation error when processing HTML redirection queries, which could be exploited to conduct cross-site scripting attacks.

CVE-2007-0938

A remote code execution vulnerability exists in Content Management Server because of the way it handles a specially crafted HTTP request that contains unexpected characters.

CVE-2007-0939

A cross-site scripting and spoofing vulnerability exists which could allow an attacker to run arbitrary code. This is caused by incomplete input validation in an HTML redirection query.

Comment:

By default IE Service 6.0 runs the W3WP.exe process as a low privilege process running as the built in network service account.

There are currently no known exploits for these vulnerabilities, however GovCertUK expect exploitation of these vulnerabilities in the near future.

References:

<http://www.microsoft.com/technet/security/bulletin/ms07-018.mspx>

<http://www.fsirt.com/english/advisories/2007/1322>

Patch Details - MS07-019

Vulnerability in Universal Plug and Play – 11th April 2007

MS07-019 Vulnerability in Universal Plug and Play Could Allow Remote Code Execution

Affected Software

Microsoft Windows 2000 Service Pack 4
Microsoft Windows Server 2003
Microsoft Windows Server 2003 Service Pack 1
Microsoft Windows Server 2003 Service Pack 2
Microsoft Windows Server 2003 for Itanium-based Systems
Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
Microsoft Windows Server 2003 with SP2 for Itanium-based Systems
Microsoft Windows Server 2003 x64 Edition
Microsoft Windows Server 2003 x64 Edition Service Pack 2
Windows Vista
Windows Vista x64 Edition

Vulnerability

CVE-2007-1204

A buffer overflow error exists in the Universal Plug and Play Service due to it failing to properly handle malformed HTTP requests.

This could be exploited by attackers to run arbitrary code.

Comment:

If exploited, an attacker would only run code in the context of the local Service account only and not under the local System account.

Firewall best practice would help mitigate the threat of this vulnerability by blocking connections to relevant ports from outside the local network.

It has been reported that proof of concept code is available for this vulnerability.

References:

<http://www.microsoft.com/technet/security/bulletin/ms07-019.mspx>

Patch Details - MS07-020

Vulnerability in Microsoft Agent – 11th April 2007

MS07-020 Vulnerability in Microsoft Agent Could Allow Remote Code Execution

Affected Software

Microsoft Windows 2000 Service Pack 4
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
Microsoft Windows Server 2003 Service Pack 1
Microsoft Server 2003 Service Pack 2
Microsoft Windows Server 2003 for Itanium-based Systems,
Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
Microsoft Windows Server 2003 with SP2 for Itanium-based Systems

Vulnerability

CVE-2007-1205

A remote code execution vulnerability exists in Microsoft Agent in the way that it handles crafted URLs. This could be exploited by an attacker to run arbitrary code in the context of the local user.

Comment

It is expected that this vulnerability will be exploited by malicious web sites, or by malicious HTML email content.

By default all supported versions of Outlook open HTML e-mail messages in the restricted sites zone. This could help reduce attacks that exploit this vulnerability via email.

Internet Explorer 7 is not affected by this vulnerability.

References:

<http://www.microsoft.com/technet/security/bulletin/ms07-020.mspx>

Patch Details - MS07-021

Vulnerabilities in CSRSS – 11th April 2007

MS07-021 Vulnerabilities in CSRSS Could Allow Remote Code Execution

Microsoft Windows 2000 Service Pack 4
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
Microsoft Windows Server 2003 Service Pack 1
Microsoft Windows Server 2003 Service Pack 2
Microsoft Windows Server 2003 (Itanium)
Microsoft Windows Server 2003 SP1 (Itanium)
Microsoft Windows Server 2003 SP2 (Itanium)
Microsoft Windows Server 2003 x64 Edition
Microsoft Windows Server 2003 x64 Edition Service Pack 2
Microsoft Windows Vista
Microsoft Windows Vista x64 Edition

CVE-2006-6696

A remote code execution vulnerability exists in the Windows Client/Server Run-time Subsystem (CSRSS) process because of the way that it handles error messages. An attacker could exploit the vulnerability by constructing a specially crafted application that could potentially allow remote code execution.

Additionally, if a user viewed a specially crafted Web site, an attacker who successfully exploited this vulnerability could take complete control of an affected system.

Comment

This vulnerability could be exploited remotely using a specially crafted web page although the attacker would need to persuade the user to visit this. Proof of concept code has been seen although there have been no signs of its use in an attack.

CVE-2007-1209

A privilege elevation vulnerability exists in the way that the Windows 32 Client/Server Run-time Subsystem (CSRSS) handles its connections during the startup and stopping of processes.

CVE-2006-6797

A denial of service vulnerability exists in the Client/Server Run-time Subsystem (CSRSS) service because of the way it handles error messages. An attacker could exploit the vulnerability by running a specially crafted application causing the system to restart.

Comment

There have been known exploits since December 15th, 2006. CVE-2007-1209 and CVE-2006-6797 are not remotely exploitable meaning that attackers would must have valid logon credentials and be able to log on locally to exploit this vulnerability.

References:

<http://www.microsoft.com/technet/security/bulletin/ms07-021.mspx>

Summary of Important Patches

Patch Details - MS07-022

Vulnerability in Windows Kernel – 11th April 2007

MS07-022 Vulnerability in Windows Kernel Could Allow Elevation of Privilege

Affected software:

Microsoft Windows 2000 Service Pack 4
Microsoft Windows XP Service Pack 2
Microsoft Windows Server 2003
Microsoft Windows Server 2003 Service Pack 1
Microsoft Windows Server 2003 Service Pack 2

CVE-2007-1206

A privilege elevation vulnerability exists in Windows Kernel because of incorrect permissions on a mapped memory segment. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Comment

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.

References:

<http://www.microsoft.com/technet/security/bulletin/ms07-022.mspx>