



Summary of Important Patches – July 2008

Microsoft Security Bulletin - MS08-037

Vulnerabilities in Windows DNS

MS08-037 Vulnerabilities in Windows DNS Could Allow Spoofing

This security update resolves two privately reported vulnerabilities in the Windows Domain Name System (DNS) that could allow spoofing. These vulnerabilities exist in both the DNS client and DNS server and could allow a remote attacker to redirect network traffic intended for the Internet to the attacker's own systems.

This security update is rated Important for all supported editions of Microsoft Windows 2000, Windows XP, Windows Server 2003, and Windows Server 2008.

The security update addresses the vulnerabilities by using strongly random DNS transaction IDs, using random sockets for UDP queries, and updating the logic used to manage the DNS cache.

Affected Software

Microsoft Windows 2000 Professional Service Pack 4
Windows XP Service Pack 2
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 Server 2008 for 32-bit Systems
Windows Server 2008 for x64-based Systems

Vulnerability Details

CVE-2008-1447

A spoofing vulnerability in Windows DNS client and Windows DNS server, caused by the Windows DNS service not providing enough entropy when performing DNS queries. This could allow a remote attacker to quickly and reliably spoof responses, and subsequently insert records into the DNS server or client cache, thereby redirecting Internet traffic.

The update removes this vulnerability by using strongly random DNS transaction ID values and random UDP sockets for remote queries.

CVE-2008-1454

A cache poisoning vulnerability exists in Windows DNS Server whereby under certain conditions, the DNS server accepts records from a response that is outside the remote server's authority. This vulnerability could allow an unauthenticated attacker to send malicious responses to DNS

Microsoft Monthly Patch Summary - Date: 8th July 2008

requests made by vulnerable systems, thereby poisoning the DNS cache and redirecting Internet traffic from legitimate locations.

The update removes the vulnerability by correcting internal DNS processing to avoid cache poisoning

Comment / Mitigation

- Microsoft has not identified any workarounds for this vulnerability.
- See <http://www.microsoft.com/technet/security/bulletin/MS08-037.msp> for relevant mitigation advice.

References:

<http://www.microsoft.com/technet/security/bulletin/MS08-037.msp>

Microsoft Security Bulletin - MS08-038

Vulnerability in Windows Explorer

MS08-038 Vulnerability in Windows Explorer Could Allow Remote Code Execution

This security update resolves a publicly reported vulnerability in Windows Explorer that could allow remote code execution when a specially crafted saved-search file is opened and saved; This operation causes Windows Explorer to exit and restart in an exploitable manner. 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. 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.

This security update is rated Important for all supported editions of Windows Vista and Windows Server 2008.

The security update addresses these vulnerabilities by modifying the way that Windows Explorer parses saved searches.

Affected Software

Windows Vista and Windows Vista SP 1
Windows Vista x64 Edition and Windows Vista x64 Edition SP 1
Windows Server 2008 for 32-bit Systems
Windows Server 2008 for x64-based Systems
Windows Server 2008 for Itanium-based Systems

Vulnerability Details

CVE-2008-1435

This is a remote code execution vulnerability that arises due to Windows Explorer not correctly parsing search files when saving them. 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. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

The security update addresses the vulnerability by modifying the way that Windows Explorer parses saved searches to correctly validate the content structure of all saved-search files.

Comment / Mitigation

- Mitigation sets 1 and 2 apply.
- There are currently no known exploits for this vulnerability; however GovCertUK recommend this patch is applied immediately.
- See <http://www.microsoft.com/technet/security/bulletin/MS08-038.msp> for relevant mitigation advice.

Microsoft Monthly Patch Summary - Date: 8th July 2008

References:

<http://www.microsoft.com/technet/security/bulletin/MS08-038.msp>

Microsoft Security Bulletin - MS08-039

Vulnerabilities in Outlook Web Access for Exchange Server

MS08-039 Vulnerabilities in Outlook Web Access Could Allow Escalation of Privileges

This important security update resolves multiple privately reported vulnerabilities in Outlook Web Access (OWA) for Microsoft Exchange Server. If successfully exploited these vulnerabilities would allow an attacker to gain access to an individual's OWA session data, resulting in an escalation of privileges. The attacker would have full control of the session and would be able to perform the same actions as the user from within OWA.

This security update is rated Important for supported editions of Microsoft Exchange Server 2003 and Microsoft Exchange Server 2007.

Affected Software

Microsoft Exchange Server 2003 Service Pack 2
Microsoft Exchange Server 2007
Microsoft Exchange Server 2007 Service Pack 1

Vulnerability Details

CVE-2008-2247

A data validation cross-site scripting (XSS) vulnerability affecting the above mentioned vulnerable versions of OWA for Microsoft Exchange Server could lead to elevation of privileges on individual clients. To successfully exploit this vulnerability an attacker must coerce a user to open a specifically crafted e-mail within OWA that would run a malicious script.

If executed, the malicious script would execute with the privileges of the user in the OWA session, allowing the attacker to send, receive and delete e-mail as the logged on user. The security patch resolves this issue by ensuring that OWA correctly validates e-mail fields when opening e-mails.

CVE-2008-2248

A HTML parsing cross-site scripting (XSS) vulnerability affecting the above mentioned vulnerable versions of OWA for Microsoft Exchange Server could lead to elevation of privileges on individual clients. To successfully exploit this vulnerability an attacker must coerce a user to open a specifically crafted e-mail within OWA that would run a malicious script.

If executed, the malicious script would execute with the privileges of the user in the OWA session, allowing the attacker to send, receive and delete e-mail as the logged on user. The security patch resolves this issue by modifying the way that OWA validates HTML when rendering e-mail.

Comment / Mitigation

- OWA Premium is not affected by this vulnerability. OWA premium is only accessible when using Internet Explorer to access OWA.
- There are currently no known exploits for this vulnerability; however GovCertUK recommend this patch is applied immediately.

Microsoft Monthly Patch Summary - Date: 8th July 2008

- See <http://www.microsoft.com/technet/security/bulletin/MS08-039.aspx> for relevant mitigation advice.

References:

<http://www.microsoft.com/technet/security/bulletin/MS08-039.aspx>

Microsoft Security Bulletin - MS08-040

Vulnerabilities in Microsoft SQL Server

MS08-040 Vulnerabilities in MS SQL Server Could Allow Elevation of Privilege

This security update resolves four privately disclosed vulnerabilities in Microsoft SQL Server. These vulnerabilities could allow an attacker to run code and to take complete control of the system. An authenticated attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

This security update is rated Important for supported releases of SQL Server 7.0, SQL Server 2000, SQL Server 2005, Microsoft Data Engine (MSDE) 1.0, Microsoft SQL Server 2000 Desktop Engine (MSDE 2000), Microsoft SQL Server 2005 Express Edition, Microsoft SQL Server 2000 Desktop Engine (WMSDE), and Windows Internal Database (WYukon).

Affected Software

SQL Server 7.0 Service Pack 4
SQL Server 2000 Service Pack 4
SQL Server 2000 Itanium-based Edition Service Pack 4
SQL Server 2005 SP 1 and SP 2
SQL Server 2005 x64 Edition SP 1 and SP 2
SQL Server 2005 with SP2 for Itanium-based Systems
Microsoft Data Engine (MSDE) 1.0
Microsoft SQL Server 2000 Desktop Engine (MSDE 2000)
Microsoft SQL Server 2005 Express Edition SP 1 and SP 2
Microsoft SQL Server 2000 Desktop Engine (WMSDE) on Windows 2000 SP 4
Microsoft SQL Server 2000 Desktop Engine (WMSDE) on Windows Server 2003 Service Pack 1 and Service Pack 2
Microsoft SQL Server 2000 Desktop Engine (WMSDE) on Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2
Windows Internal Database (WYukon) Service Pack 2 on Windows Server 2003 Service Pack 1 and Service Pack 2
Windows Internal Database (WYukon) x64 Edition Service Pack 2 on Windows Server 2003 x64 Edition and Service Pack 2
Windows Internal Database (WYukon) Service Pack 2 on Windows Server 2008 for 32-bit Systems
Windows Internal Database (WYukon) x64 Edition Service Pack 2 on Windows Server 2008 for x64-based Systems

Vulnerability Details

CVE-2008-0085

When reallocating memory, SQL Server fails to initialise memory pages, resulting in an information disclosure vulnerability.

This vulnerability requires that an attacker have database operator access to the database, log, database backup files, or log backup files. An attacker with database operator access could assemble the uninitialised memory pages from another user's session by directing a backup to a location that the attacker controls.

The update removes the vulnerability by modifying the way that SQL Server manages page reuse.

CVE-2008-0086

An elevation of privilege vulnerability exists in the way that SQL Server converts SQL expressions from one data type to another.

The convert function in SQL Server improperly checks input strings before passing them to the buffer. As a result, an unchecked buffer overrun is possible, allowing an authenticated attacker to create a query that calls the convert function with a specially crafted expression, causing the function to overflow and allowing code execution.

An attacker who successfully exploited this vulnerability could run code and take complete control of the system.

The update eliminates the vulnerability by allocating more memory for the convert function.

CVE-2008-0107

A vulnerability exists where SQL Server data structures are not sufficiently validated on disk files. As a result, an unchecked buffer overrun is possible, allowing an authenticated attacker to run code and to take complete control of the system, e.g. by creating a malicious file and force SQL to load the file. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

The update eliminates the vulnerability by validating on-disk files before loading.

CVE-2008-0106

An elevation of privilege vulnerability exists in the way that SQL Server manages memory in processing the insert statement, i.e. this vulnerability could allow an authenticated attacker to create insert statements that cause a buffer overrun run code and to take complete control of the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

An authenticated attacker could, thus corrupting memory.

The update eliminates the vulnerability by validating insert statements

Comment / Mitigation

- See <http://www.microsoft.com/technet/security/bulletin/MS08-040.msp> for relevant mitigation advice.
- There are currently no known exploits for these vulnerabilities; however GovCertUK recommend this patch is applied immediately.

References:

<http://www.microsoft.com/technet/security/bulletin/MS08-040.msp>

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.