

[NT] Vulnerabilities in DNS Allows Spoofing (MS08-037)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-07/msg00012.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 9 Jul 2008 14:42:32 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Vulnerabilities in DNS Allows Spoofing (MS08-037)

SUMMARY

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 systems on 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. For more information, see the subsection, Affected and Non-Affected Software, in this section.

DETAILS

Affected Software:

*

<<http://www.microsoft.com/downloads/details.aspx?familyid=269c219c-9d6b-4b12-b621-c70cd07cdd22>>

Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?familyid=332aa92f-a1ad-42a0-87d0-485d2d41335b>>

Microsoft Windows 2000 Server Service Pack 4 – Spoofing – Important – None

[NT] Vulnerabilities in DNS Allows Spoofing (MS08-037)

*

<<http://www.microsoft.com/downloads/details.aspx?familyid=ed989a33-7a9e-4423-93a8-b38907467cdf>>
Windows XP Service Pack 2 and Windows XP Service Pack 3 – Not applicable – Spoofing – Important – None

*

<<http://www.microsoft.com/downloads/details.aspx?familyid=a2b016fa-b108-4e8e-b41b-4ca89002907b>>
Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 – Not applicable – Spoofing – Important – None

*

<<http://www.microsoft.com/downloads/details.aspx?familyid=4ef5033c-9843-4e0b-bfad-fcaf05d7dab9>>
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?familyid=d1fcb794-e6a5-4c28-b3b3-9cd88f468a42>>
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 – Spoofing – Important – None

*

<<http://www.microsoft.com/downloads/details.aspx?familyid=66624a1f-38bf-4af7-936d-3131474ffe1f>>
Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?familyid=040a1ba8-21b0-439e-bf21-1acd1c43b162>>
Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2 – Spoofing – Important – None

*

<<http://www.microsoft.com/downloads/details.aspx?familyid=facc80da-61d6-49c5-872d-a1980b66ae3e>>
Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?familyid=c63e3ee6-6055-4313-b0f1-fec7408886bb>>
Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems – Spoofing – Important – None

* Not applicable –

<<http://www.microsoft.com/downloads/details.aspx?familyid=1fcea8f4-b233-42e1-b913-c4fcae276c7b>>
Windows Server 2008 for 32-bit Systems* – Spoofing – Important – None

* Not applicable –

<<http://www.microsoft.com/downloads/details.aspx?familyid=afac5bbc-71fa-457b-8b0a-f5902d37bfd0>>
Windows Server 2008 for x64-based Systems* – Spoofing – Important – None

*Windows Server 2008 server core installation affected. For supported editions of Windows Server 2008, this update applies, with the same severity rating, whether or not Windows Server 2008 was installed using the Server Core installation option. For more information on this installation option, see Server Core. Note that the Server Core installation option does not apply to certain editions of Windows Server 2008; see Compare Server Core Installation Options.

Non-Affected Software:

* Windows Vista and Windows Vista Service Pack 1

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

* Windows Server 2008 for Itanium-based Systems

*Windows Server 2008 server core installation affected. For supported editions of Windows Server 2008, this update applies, with the same severity rating, whether or not Windows Server 2008 was installed using the Server Core installation option.

[NT] Vulnerabilities in DNS Allows Spoofing (MS08-037)

DNS Insufficient Socket Entropy Vulnerability – CVE-2008-1447

A spoofing vulnerability exists in Windows DNS client and Windows DNS server. This vulnerability could allow a remote unauthenticated attacker to quickly and reliably spoof responses and insert records into the DNS server or client cache, thereby redirecting Internet traffic.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1447>>
CVE-2008-1447

DNS Cache Poisoning Vulnerability – CVE-2008-1454

A cache poisoning vulnerability exists in Windows DNS Server. The vulnerability could allow an unauthenticated remote attacker to send specially crafted responses to DNS requests made by vulnerable systems, thereby poisoning the DNS cache and redirecting Internet traffic from legitimate locations.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1454>>
CVE-2008-1454

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/ms08-037.msp>>
<http://www.microsoft.com/technet/security/bulletin/ms08-037.msp>

=====
This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.