

[NT] Vulnerability in DNS Client Allows Spoofing (MS08-020)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-04/msg00022.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 9 Apr 2008 09:04:20 +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>

Vulnerability in DNS Client Allows Spoofing (MS08-020)

SUMMARY

This security update resolves a privately reported vulnerability. This spoofing vulnerability exists in Windows DNS clients and could allow an attacker to send specially crafted responses to DNS requests, thereby spoofing or redirecting Internet traffic from legitimate locations.

This is an important security update for Windows Vista and all supported editions of Microsoft Windows 2000, Windows XP, and Windows Server 2003. For more information, see the subsection, Affected and Non-Affected Software, in this section.

DETAILS

Affected Software:

Operating System – Maximum Security Impact – Aggregate Severity Rating –
Bulletins Replaced by This Update

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=41326ade-96b6-47ce-9291-d4e3039471c4>>

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

*

[NT] Vulnerability in DNS Client Allows Spoofing (MS08-020)

<<http://www.microsoft.com/downloads/details.aspx?FamilyID=893f4cef-0395-4c44-ba28-7a10b6e7dd48>>
Windows XP Service Pack 2 – Spoofing – Important – None

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyID=8fdd1207-6e93-4c43-bacc-fe3623a6ebe7>>
Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 – Spoofing – Important – None

* W

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=214bd8f5-6eb2-414c-b013-c516a306d692>>
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 – Spoofing – Important – None

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=fd123394-a5d6-4b55-be74-2938f52ce922>>
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=e0e63f03-904d-47ee-94fc-51a8dea668eb>>
Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems – Spoofing – Important – None

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyID=8203d303-c855-4579-9bbf-b06ddf5c1b87>>
Windows Vista – Spoofing – Important – None

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyID=73f3a234-3973-4467-be7e-69efa7ee978c>>
Windows Vista x64 Edition – Spoofing – Important – None

Non-Affected Software:

* Windows Vista Service Pack 1 (all editions)

* Windows Server 2008 (all editions)

DNS Spoofing Attack Vulnerability – CVE-2008-0087

A spoofing vulnerability exists in Windows DNS clients. The vulnerability could allow an unauthenticated attacker to send malicious responses to DNS requests made by vulnerable clients, thereby spoofing or redirecting Internet traffic from legitimate locations.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0087>>
CVE-2008-0087

FAQ for DNS Spoofing Attack Vulnerability – CVE-2008-0087

What is the scope of the vulnerability?

A spoofing vulnerability exists in Windows DNS Clients. An attacker who successfully exploited this vulnerability could impersonate a legitimate address.

What causes the vulnerability?

The Windows DNS Client service doesn't provide enough entropy in its random choice of transaction values when performing DNS queries.

What might an attacker use the vulnerability to do?

An attacker who has successfully gained information about DNS client transaction IDs could use that information to send malicious responses to

[NT] Vulnerability in DNS Client Allows Spoofing (MS08–020)

DNS requests.

How could an attacker exploit the vulnerability?

An attacker who successfully exploited this vulnerability could respond to a DNS query with false or misleading information, thereby redirecting Internet traffic from legitimate locations to an address of the attacker's choice.

What is the Domain Name System (DNS)?

Domain Name System (DNS) is one of the industry-standard suite of protocols that comprise TCP/IP. DNS is implemented using two software components: the DNS server and the DNS client (or resolver). Both components are run as background service applications. Network resources are identified by numeric IP addresses, but these IP addresses are difficult for network users to remember. The DNS database contains records that map user-friendly alphanumeric names for network resources to the IP address used by those resources for communication. In this way, DNS acts as a mnemonic device, making network resources easier to remember for network users. For more information and to view logical diagrams illustrating how DNS fits with other Windows technologies, review the article [How DNS Works](#).

Could the vulnerability be exploited over the Internet?

Yes, an attacker could exploit this vulnerability over the Internet by sending specific responses to an Internet-facing client system that is performing DNS queries.

What systems are primarily at risk from the vulnerability?

Any Windows system that is connected to the Internet or another network populated by potentially hostile users would be at risk. Windows XP Service Pack 3, Windows Vista SP1, and Windows Server 2008 are not affected by this vulnerability.

What does the update do?

The update removes this vulnerability by increasing the randomness of the transaction IDs in DNS client communications.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

ADDITIONAL INFORMATION

[NT] Vulnerability in DNS Client Allows Spoofing (MS08-020)

The information has been provided by Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS08-020.msp>>

<http://www.microsoft.com/technet/security/Bulletin/MS08-020.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@xxxxxxxxxxxxxx

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

=====

=====

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.