

[NT] TCP/IP IGMP DoS (MS06-007)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00052.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 15 Feb 2006 11:45:16 +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>

TCP/IP IGMP DoS (MS06-007)

SUMMARY

A specially crafted IGMP packet sent to a vulnerable system could create a <<http://go.microsoft.com/fwlink/?LinkId=21142x>> denial of service situation and cause the system to stop responding.

DETAILS

Vulnerable Systems:

* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=7BB21D74-C37B-472B-BB10-71D4680680A7>>

Download the update

* Microsoft Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8E2538CC-CC90-4DB7-8D0B-0B8BA4234E67>>

Download the update

* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=78D7DF14-6049-4318-89CA-9C8681CED8AB>>

Download the update

* Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems

[NT] TCP/IP IGMP DoS (MS06-007)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9AE276CF-AB46-4198-BCB3-3EFFDF15550E>>

Download the update

* Microsoft Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=12AAE69E-C5C3-4E4A-9970-F5DB84DD9744>>

Download the update

* Note The security updates for Microsoft Windows Server 2003, Microsoft Windows Server 2003 Service Pack 1, and Microsoft Windows Server 2003 x64 Edition also apply to Microsoft Windows Server 2003 R2.

Immune Systems:

* Microsoft Windows 2000 Service Pack 4

* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

Mitigating Factors for IGMP v3 DoS Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0021>>

CVE-2006-0021:

Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

Note Windows Firewall will help protect against attacks utilizing a unicast IGMP v3 packet, however, it will not help protect against an attack utilizing a multicast IGMP v3 packet.

Workarounds for IGMP v3 DoS Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0021>>

CVE-2006-0021:

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

Disable IGMP

Disabling IGMP will prevent an affected host from processing IGMP related packets that could cause a system to stop responding. IGMP processing can be disabled by following these steps:

Note Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. For information about how to edit the registry, view the "Changing Keys And Values" Help topic in Registry Editor (Regedit.exe) or view the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe.

Note We recommend backing up the registry before you edit it.

1. Click Start, click Run, type "regedit32 " (without the quotation marks), and then click OK.

2. In Registry Editor, locate the following registry key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\
3. Add the DWORD Value: IGMPLevel. Set the value to 0. This value disables IGMP processing. By default, this key does not exist.
4. You must restart your system for this change to take effect.

Block all IGMP network packets at the firewall or router

Blocking IGMP packets at the firewall or at the router will help protect systems that are behind that firewall or router from attempts to exploit this vulnerability. We recommend that you block all unsolicited inbound communication from the Internet. ISA Server 2000 and ISA Server 2004 can be used to block the affected types of traffic.

Impact of Workaround: These changes will help prevent attacks by restricting the ability of an attacker to send malformed IGMP packets to the affected host. This setting can also negatively impact network performance and communication by preventing the ability of routers to properly forward packets between subnets.

Note Windows Firewall will help protect against attacks utilizing a unicast IGMP v3 packet, however, it will not help protect against an attack utilizing a multicast IGMP v3 packet.

FAQ for IGMP v3 DoS Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0021>>
CVE-2006-0021:

What is the scope of the vulnerability?

This is a <<http://go.microsoft.com/fwlink/?LinkId=21142>> denial of service vulnerability. An attacker who exploited this vulnerability could cause the affected system to stop responding. During that time, the server cannot respond to requests. Note that the denial of service vulnerability would not allow an attacker to execute code or to elevate their user rights, but it could cause the affected system to stop accepting requests.

What causes the vulnerability?

The affected messages are not being ignored in certain cases that allow an attacker to send a malformed packet which may cause affected system to stop responding.

What is IGMP?

Internet Group Management Protocol (IGMP) is a TCP/IP standard defined in RFC 1112 "Internet Group Management Protocol (IGMP)." In addition to defining address and host extensions for how IP hosts support multicasting, this RFC also defines the Internet Group Management Protocol (IGMP) version 1. RFC 2236, "Internet Group Management Protocol (IGMP), version 2" defines IGMP version 2. Both versions of IGMP provide a protocol to exchange and update information about host membership in specific multicast groups. Additionally, the Windows Server 2003 family supports IGMP version 3, described in the Internet Draft titled "Internet Group Management Protocol, version 3." With IGMP version 3, hosts can specify interest in receiving multicast traffic from specified sources or

[NT] TCP/IP IGMP DoS (MS06-007)

from all but a specific set of sources. For more information about IGMP, visit the Microsoft Tech Net

<<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/ffa6231a-bf9b-4691-a63d-9>>
Web site.

Who could exploit the vulnerability?

Any anonymous user who could deliver a specially crafted message to the affected system could try to exploit this vulnerability.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system. The message could then cause the affected system to stop responding.

What systems are primarily at risk from the vulnerability?

Workstations and Servers are both potentially at risk from this vulnerability.

Could the vulnerability be exploited over the Internet?

Yes. An attacker could try to exploit this vulnerability over the Internet. Firewall best practices and standard default firewall configurations can help protect against attacks that originate from the Internet. Microsoft has provided information about how you can help protect your PC. End users can visit the <<http://go.microsoft.com/fwlink/?LinkId=21169>> Protect Your PC Web site. IT professionals can visit the <<http://go.microsoft.com/fwlink/?LinkId=21171>> Security Guidance Center Web site.

What does the update do?

The update removes the vulnerability by modifying the way that the affected operating systems validate IGMP requests.

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

The information has been provided by Microsoft Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS06-007.msp>>

[NT] TCP/IP IGMP DoS (MS06-007)

<http://www.microsoft.com/technet/security/Bulletin/MS06-007.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@xxxxxxxxxxxxxxx

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

=====

=====

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.