

[NT] Flaw in Winsock Proxy Service and ISA Firewall Service Can Cause Denial of Service

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-04/0013.html>

From: support@securiteam.com

Date: 04/12/03

From: support@securiteam.com

To: list@securiteam.com

Date: 12 Apr 2003 21:22:13 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Flaw in Winsock Proxy Service and ISA Firewall Service Can Cause Denial of Service

SUMMARY

Microsoft Proxy Server 2.0 and Microsoft Internet Security and Acceleration (ISA) Server 2000 contain support for Windows Sockets (Winsock) proxy communications. Winsock is an API that handles communications requests for Internet applications in a Microsoft Windows operating system.

The Winsock proxy service works with FTP, Telnet, mail, news, Internet Relay Chat (IRC), and other client applications that are compatible with Winsock. The proxy service makes these applications perform as if they were directly connected to the Internet. The service redirects the necessary communications functions to a computer that is running either Proxy Server 2.0 or ISA Server. This establishes a communication path from the internal application to the Internet.

A flaw in the Winsock Proxy service allows users from the internal network to cause a Denial-of-Service condition on Microsoft proxy and on ISA

Securiteam: [NT] Flaw in Winsock Proxy Service and ISA Firewall Service Can Cause Denial of Service

server.

DETAILS

There is a flaw in the Winsock Proxy service in Microsoft Proxy Server 2.0, and the Microsoft Firewall service in ISA Server 2000, that would allow an attacker on the internal network to send a specially crafted packet that would cause the server to stop responding to internal and external requests. Receipt of such a packet would cause CPU utilization on the server to reach 100%, and thus make the server unresponsive. The Winsock Proxy service and Microsoft Firewall service work with FTP, telnet, mail, news, Internet Relay Chat (IRC), or other client applications that are compatible with Windows Sockets (Winsock). These services allow these applications to perform as if they were directly connected to the Internet. These services redirect the necessary communications functions to a Proxy Server 2.0 or ISA Server computer, thus establishing a communication path from the internal application to the Internet through it.

Mitigating factors:

The vulnerability would not enable an attacker to gain any privileges on an affected Proxy Server 2.0 or ISA Server computer or compromise any cached content. It is strictly a denial of service.

ISA Server computers running in cache mode are not affected because the Microsoft Firewall service is disabled by default.

Patch:

Patch can be found at:

<<http://support.microsoft.com/default.aspx?scid=kb;en-us:331066>>
<http://support.microsoft.com/default.aspx?scid=kb;en-us:331066>

ADDITIONAL INFORMATION

The original Microsoft security advisory can be found at:

<<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-012.asp>>
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-012.asp>

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

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

Securiteam: [NT] Flaw in Winsock Proxy Service and ISA Firewall Service Can Cause Denial of Service

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