

[NEWS] Proxy Vulnerability in TrendMicro InterScan VirusWall

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0027.html>

From: support@securiteam.com

Date: 12/08/02

From: support@securiteam.com

To: list@securiteam.com

Date: 8 Dec 2002 23:11:47 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Proxy Vulnerability in TrendMicro InterScan VirusWall

SUMMARY

A quite well known type of proxy vulnerability was found for TrendMicro's InterScan VirusWall. This general problem has been known to be an issue with plain HTTP proxies like Squid.

DETAILS

Vulnerable systems:

- * TrendMicro's InterScan VirusWall version 3.6

Immune systems:

- * TrendMicro's InterScan VirusWall version 3.7 Build 1190 or newer

The vulnerability can be exploited using the CONNECT method to connect to a different server, e.g. an internal mailserver.

Example:

You = 6.6.6.666

Trendmicro ISVW = 1.1.1.1 (HTTP proxy at port 80)

Internal Mailserver = 2.2.2.2

Securiteam: [NEWS] Proxy Vulnerability in TrendMicro InterScan VirusWall

Connect with "telnet 1.1.1.1 80" to ISVW proxy and enter: CONNECT
2.2.2.2:25 / HTTP/1.0

The response should be the mail server banner.

You can connect to any TCP port on any machine the proxy can connect to.
Telnet, SMTP, POP, etc.

Solution:

Update to ISVW 3.7 Build 1190 or newer (available since some weeks now).

Workarounds:

- Disable the HTTP proxy.
- You have a firewall that prevents unauthorized access to the Trend ISVW proxy.

ADDITIONAL INFORMATION

The information has been provided by <mailto:volker.tanger@discon.de>
Volker Tanger.

=====

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.

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