

[NEWS] NetScreen SSH1 CRC32 Denial of Service

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0004.html>

From: support@securiteam.com

Date: 11/03/02

From: support@securiteam.com

To: list@securiteam.com

Date: 3 Nov 2002 13:07:07 +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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

NetScreen SSH1 CRC32 Denial of Service

SUMMARY

<<http://www.netscreen.com/>> NetScreen Technologies are the manufacturers of some of the industry's highest quality VPN and firewall equipment. The NetScreen product has been found to be vulnerable to the SSH1 CRC32 attack.

DETAILS

In February of 2001, BindView's RAZOR Team announced the SSH1 CRC32 compensation attack detector bug. After all was said and done, several vendors found their SSH implementations were vulnerable.

By default the NetScreen does not ship with SSH enabled, and NetScreen usually doesn't encourage their customers to even access the CLI on their devices. However, in the GUI you can enable SSH, and disable telnet. This only opens SSH on the trusted interfaces, unless you specifically add rules to forward to this interface/port. On a normal system with SSH enabled, the unit will only be vulnerable to attackers on the trusted side.

If you use any of the CRC32 exploits out there, the unit will crash immediately, and require a hard reboot. It does not appear from our analysis that anything more than a crash can occur from this.

Securiteam: [NEWS] NetScreen SSH1 CRC32 Denial of Service

Vendor response:

As a temporary solution until NetScreen can release a new ScreenOS, you could disable SSH if this is a viable option for you.

So, it would appear NetScreen did NOT miss the CRC32 bugs that came out, and it's just a new one.

ADDITIONAL INFORMATION

The information has been provided by
<mailto:erik.parker@digitaldefense.net> Erik Parker of Digital Defense,
Inc.

=====

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.

-
- *Previous message:* support@securiteam.com: "[\[UNIX\] Buffer Overflow Vulnerability in Abuse](#)"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)