

[NEWS] NetScreen TCP Option DoS (manager-ip)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0003.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/01/03

To: list@securiteam.com

Date: 1 Aug 2003 01:07:26 +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

Get Thawte's New Step-by-Step SSL Guide for Apache.

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on you Apache web server.

Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get you copy of this new guide now:

<http://ad.doubleclick.net/clk;5903117;8265118;i>

NetScreen TCP Option DoS (manager-ip)

SUMMARY

A malicious user connecting to a NetScreen Security Device with a certain TCP option set can cause it to reboot, causing a temporary service outage.

DETAILS

Vulnerable systems:

- * NetScreen Firewall/VPN products running ScreenOS 4.0.1r1 through 4.0.1r6 and 4.0.3r1 and 4.0.3r2

Immune systems:

- * NetScreen IDP, NetScreen Firewall/VPN products running ScreenOS 3 and below, 4.0.0, 4.0.1r7 and higher, 4.0.2, 4.0.3r3 and higher

Due to a bug in ScreenOS, a non-privileged user who attempts to connect to a NetScreen Security Device management IP from the range of addresses permitted by the manager-ip feature with a particular TCP Window option setting can cause the system to crash and reboot. This issue affects Telnet and WebUI (HTTP/HTTPS) management, as well as WebAuth

Securiteam: [NEWS] NetScreen TCP Option DoS (manager-ip)

authentication service (HTTP/HTTPS).

SSH management connections to the NetScreen device are not susceptible, nor are the classic policy-driven firewall authentication (ProxyAuth) connections. Additionally, traffic passing through the device does not crash the device, only particular TCP sessions terminating on the device itself.

Recommended Actions:

Restrict administrative access to known administrator hosts and/or subnets with the 'set admin manager-ip ...' feature.

Activate ScreenOS' anti-spoofing feature to prevent spoofed manager IP's from non-manager subnets.

Turn off management on all interfaces not facing the IT management network (NOC/SOC/etc).

Use ProxyAuth instead of WebAuth for policy authentication.

Use SSH instead of Telnet to remotely manage your NetScreen firewall.

Upgrade to maintenance release r7 or later of ScreenOS 4.0.1, or maintenance release r3 or later of ScreenOS 4.0.3.

ADDITIONAL INFORMATION

Please refer to the following URL for more information:

<http://www.netscreen.com/services/security/alerts/advisory-57739.txt>
<http://www.netscreen.com/services/security/alerts/advisory-57739.txt>

The information has been provided by

security-alert@netscreen.com NetScreen Security Response Team.

=====

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.