

[NEWS] NetScreen non-IP Protocol Denial of Service (And non-IP Machine Compromise)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0123.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/28/03

To: list@securiteam.com

Date: 28 Jul 2003 18:36:11 +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.

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

NetScreen non-IP Protocol Denial of Service (And non-IP Machine Compromise)

SUMMARY

Transparent Mode is the factory-default mode for the NetScreen 25, 50, 204 and 208 appliances, and the NetScreen 500, 5200, and 5400 systems. NetScreen devices in this mode of operation do not participate in IP forwarding, but instead forward packets within the same broadcast domain, somewhat as a bridge would. This allows the device to be placed transparently into an existing network between, for example, a perimeter router and its previously adjacent switch, and protect the network without requiring any network renumbering.

A malicious user adjacent to the transparent mode firewall can transmit layer 2 multicasts or broadcasts that do not contain IPv4 frames and potentially adversely affect hosts on the other side of the firewall. Examples would be injecting arbitrary Netware SAPs to poison IPX hosts or consume all of their storage reserved for this; injecting BPDUs to force MAC-layer switches to rebalance the spanning tree; etc.

The possibility of this threat is only present if the NetScreen device is in Transparent Mode, and only if the malicious user is within the same broadcast domain as the NetScreen device.

Securiteam: [NEWS] NetScreen non-IP Protocol Denial of Service (And non-IP Machine Compromise)

In general, Internet Service Providers only provide IP transport, so that side of the firewall is only vulnerable to immediately adjacent devices sending non-IP broadcasts or multicasts. Such devices would need to gain physical access to the broadcast domain directly connected to the NetScreen device.

DETAILS

Affected Products:

Hosts protected by NetScreen products running ScreenOS 4.0.0 or later in Transparent Mode

In transparent mode, no forwarding of any traffic will occur until/unless the administrator defines the first security policy. Once at least one security policy is defined, the device will permit layer 2 broadcasts and multicasts containing non-IPv4 frames to traverse the device in order for devices on either side of the NetScreen device to learn of each other's presence.

Layer 2 broadcasts and multicasts containing non-IPv4 frames are permitted to traverse the NetScreen devices to facilitate service advertisements, spanning tree announcements, delivery of non-routable LAN traffic, and the like.

By default, the only unicasts that can traverse the device are IPv4 unicasts, and then only according to policy. At the administrator's option, the device may be configured to permit non-IPv4 unicasts to be forwarded across the device. This is a global setting and affects all security zones and VSYS.

No inspection or policy will be applied to the non-IP unicasts, multicasts, or broadcasts.

A malicious user adjacent to the transparent mode firewall can transmit layer 2 multicasts or broadcasts containing non-IPv4 frames and potentially adversely affect hosts on the other side of the firewall. Such transmissions will traverse the NetScreen device regardless of the "set | unset firewall bypass-non-ip" setting. Examples would be injecting arbitrary Netware SAPs to poison IPX hosts or consume all of their storage reserved for this; injecting BPDUs to force MAC-layer switches to rebalance the spanning tree; etc.

Further, a malicious user one or more non-IPv4 router hops away can potentially adversely affect other hosts using non-IPv4 unicast traffic if the command "unset firewall bypass-non-ip" had previously been issued on the NetScreen device.

Most NetScreen devices are deployed as perimeter security and connect to Internet gateways. In general, Internet Service Providers only provide IP transport, so that side of the firewall is only vulnerable to immediately adjacent devices sending layer 2 broadcasts or multicasts. Such devices

Securiteam: [NEWS] NetScreen non-IP Protocol Denial of Service (And non-IP Machine Compromise)

would need to gain physical access to the broadcast domain directly connected to the NetScreen device.

Only NetScreen devices placed in a network carrying non-IPv4 traffic will be susceptible to the above threats, and then only if the NetScreen device is in transparent mode.

NetScreen will post maintenance releases to ScreenOS 4.0.1 and 4.0.3 the week of July 14 that will provide administrative control over the forwarding of non-IPv4 non-unicasts while in transparent mode. All future releases of ScreenOS will also provide administrative control over forwarding of non-IPv4 non-unicasts in transparent mode.

Recommended Actions:

Examine your network topology to determine if you must enable forwarding of non-IPv4 unicasts in your NetScreen devices and only enable it if you must.

If possible, only attach routers directly to the NetScreen device, or if you must attach end-systems via L2 switches, ensure that routers with appropriate access controls and filters act as boundaries for the non-IPv4 broadcast/multicast domains.

Upgrade to maintenance release r9 of ScreenOS 4.0.1 or maintenance release r3 of ScreenOS 4.0.3 when they are available.

How to Get ScreenOS:

If you have registered your product with NetScreen and have a valid service contract, you can simply download the software from:

<http://www.netscreen.com/services/download_soft/>

http://www.netscreen.com/services/download_soft/ or

<<http://www.netscreen.com/support/updates.html>>

<http://www.netscreen.com/support/updates.html>

Select your NetScreen device from the "Select Your Product" pull down menu. You will be prompted for your User ID and Password. Enter the whole or part of your company name as your User ID and enter your registered NetScreen device serial number as the password.

If you have not yet registered your product with NetScreen, you will need to contact NetScreen Technical Support for special instructions on how to obtain the fixed software. NetScreen Technical Support can be reached from 8 a.m. to 5 p.m. pacific time Monday through Friday excluding weekends and observed holidays. You may contact them via email at:

<<mailto:mailto:customeroperations@netscreen.com>>

customeroperations@netscreen.com or via phone at: 408.730.6000 or 800.638.8296

Please reference this Advisory title as evidence of your entitlement to the fixed software version.

Securiteam: [NEWS] NetScreen non-IP Protocol Denial of Service (And non-IP Machine Compromise)

NetScreen authorized Value Added Resellers have access to NetScreen software versions and may also be a channel through which to obtain the new release.

ADDITIONAL INFORMATION

The information has been provided by NetScreen.

=====

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.