

[NEWS] Crafted Packet Causes Reload on Cisco Routers

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0121.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/26/05

To: list@securiteam.com

Date: 26 Jan 2005 19:18:04 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Crafted Packet Causes Reload on Cisco Routers

SUMMARY

Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces. A system that supports MPLS is vulnerable even if that system is not configured for MPLS.

The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

Cisco has made free software available to address this vulnerability.

There are workarounds available to mitigate the effects.

DETAILS

Affected Products:

Vulnerable Products

Only the following products running a vulnerable version of IOS that support MPLS are affected.

Securiteam: [NEWS] Crafted Packet Causes Reload on Cisco Routers

- * 2600 and 2800 series routers
- * 3600, 3700 and 3800 series routers
- * 4500 and 4700 series routers
- * 5300, 5350 and 5400 series Access Servers

Products that are not listed above are not affected.

MPLS is not supported in IP and IP Plus feature sets. Therefore, products running an IOS version with an IP or IP Plus feature set are not vulnerable.

An attack can only be launched at systems that are not configured for MPLS Traffic Engineering and on the interfaces where MPLS is not enabled. MPLS enabled interfaces can be determined by the show mpls interfaces command.

An unaffected system where MPLS is not supported will give an output similar to the following.

```
Router#show mpls interfaces
      ^
% Invalid input detected at '^' marker.
```

Router#

MPLS can be enabled in different ways on a router. In the below output, a router is shown that has MPLS enabled for IP on interface Ethernet0/0.

```
Router#show mpls interfaces
Interface IP Tunnel Operational
Ethernet0/0 Yes (tdp) No Yes
Router#
```

When MPLS for IP is enabled on an interface, the router is immune to the attacks coming from that interface but vulnerable to the attacks coming from other interfaces. Enabling MPLS for IP on all interfaces of the router will make the router immune to attacks coming from any interface. An interface that has MPLS for IP enabled will have mpls ip or tag-switching ip command in the interface configuration.

MPLS Traffic Engineering (TE) provides a better protection against this vulnerability. If MPLS TE is enabled globally, the router will be immune to the attacks coming from any interface. A router that has MPLS TE enabled will have mpls traffic-eng tunnels command in the show running-config output.

Products Confirmed Not Vulnerable

- * Products that are not running Cisco IOS are not vulnerable.
- * Products running Cisco IOS versions 12.0 and earlier and 12.1 mainline are not vulnerable.
- * Products that are not mentioned in the Affected Products section are not vulnerable (including but not limited to Cisco 7200, 7500, 12000)

Securiteam: [NEWS] Crafted Packet Causes Reload on Cisco Routers

series and Catalyst systems).

No other Cisco products are currently known to be affected by these vulnerabilities.

Details:

Multi Protocol Label Switching (MPLS) is a vendor-independent protocol that integrates layer-2 (as defined in the Open System Interconnection Reference Model) information into layer-3. More information on MPLS can be found at <<http://www.cisco.com/warp/public/732/Tech/mpls>>
<http://www.cisco.com/warp/public/732/Tech/mpls>.

A vulnerability exists in the processing of an MPLS packet that is received on an interface where MPLS is disabled. A router that is configured for MPLS Traffic Engineering is immune to attacks coming from any interface.

A Cisco device receiving a crafted packet on an MPLS disabled interface will reset and may take several minutes to become fully functional. This vulnerability may be exploited repeatedly resulting in an extended DoS attack. This issue is documented in bugs ID CSCeb56909 (registered customers only) and CSCec86420 (registered customers only) .

Such crafted packets can only be sent from the local network segment.

Software Versions and Fixes:

A table listing all the vulnerable versions and their corresponding fixes can be found at:

<<http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml#software>>
<http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml#software>

Workarounds:

The effectiveness of any workaround is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround is the most appropriate for use in the intended network before it is deployed.

Warning: Using this workaround may affect the operation of your network and might cause problems. Therefore it is strongly recommended that you do a code upgrade if you are affected. It is not recommended that you use the workaround as a long term solution.

Enabling MPLS Traffic Engineering (MPLS TE) globally can be used as a workaround to mitigate this vulnerability. Since MPLS requires Cisco Express Forwarding (CEF) in order to work, CEF needs to be enabled first in order to enable MPLS TE.

CEF and MPLS TE can be enabled by the following commands.

Securiteam: [NEWS] Crafted Packet Causes Reload on Cisco Routers

```
Router(config)# ip cef
Router(config)# mpls traffic-eng tunnels
```

Having MPLS TE enabled will make the router immune to the attacks coming from any interface.

ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@cisco.com> Cisco Systems Product Security Incident Response Team.

The original article can be found at:

<<http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml>>
<http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml>

=====

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.