

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)[Security Advisories](#)

Cisco Security Advisory: Crafted Packet Causes Reload on Cisco Routers

Document ID: 63846

Revision 1.1

Last Updated 2005 January 28 1800 (GMT)

For Public Release 2005 January 26 1600 (GMT)

Please provide your [feedback](#) on this document.

Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Impact](#)
- [Software Versions and Fixes](#)
- [Obtaining Fixed Software](#)
- [Workarounds](#)
- [Exploitation and Public Announcements](#)
- [Status of This Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

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 interfaces where MPLS is not configured. 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.

This issue is tracked by CERT/CC VU#583638.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml>.

Affected Products

Vulnerable Products

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

- 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 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>.

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.

Impact

Successful exploitation of this vulnerability could result in a reload of the device. Repeated exploitation could result in a sustained DoS attack.

Software Versions and Fixes

Major Release	Availability of Repaired Releases	
	Rebuild	Maintenance
Affected 12.1-Based Release		
12.1DB	Migrate to 12.3(4)T or later	
12.1DC	Migrate to 12.3(4)T or later	
12.1T	Migrate to 12.2 or later	
12.1XG	Migrate to 12.3 or later	
12.1XI	Migrate to 12.2 or later	

12.1XJ	Migrate to 12.3 or later	
12.1XL	Migrate to 12.3 or later	
12.1XM	Migrate to 12.3 or later	
12.1XP	Migrate to 12.3 or later	
12.1XQ	Migrate to 12.3 or later	
12.1XR	Migrate to 12.3 or later	
12.1XT	Migrate to 12.3 or later	
12.1XU	Migrate to 12.3 or later	
12.1XV	Migrate to 12.3 or later	
12.1YA	Migrate to 12.3 or later	
12.1YB	Migrate to 12.3 or later	
12.1YC	Migrate to 12.3 or later	
12.1YD	Migrate to 12.3 or later	
12.1YE	Migrate to 12.3 or later	
12.1YF	Migrate to 12.3 or later	
12.1YH	Migrate to 12.3 or later	
12.1YI	Migrate to 12.3 or later	
Affected 12.2- Based Release	Rebuild	Maintenance
12.2	12.2(10g)	
	12.2(13e)	
	12.2(16f)	
	12.2(17d)	
	12.2(19b)	
	12.2(21a)	
		12.2(23)
12.2B	12.2(2)B through 12.2(4)B7, Migrate to 12.3 or later	
	12.2(4)B8 and forward, Migrate to 12.3(4)T or later	
12.2BC	12.2(15)BC2	
12.2BW	Migrate to 12.3 or later	
12.2BX	Migrate to 12.3(7)XI1 or later	
12.BY	Migrate to 12.3(4)T or later	
12.2BZ	Migrate to 12.3(7)XI1 or later	

12.2CX	Migrate to 12.2(15)BC2	
12.2CY	Migrate to 12.2(15)BC2	
12.2CZ	12.2(15)CZ	
12.2DA	12.2(12)DA6	
12.2DD	Migrate to 12.3(4)T or later	
12.2DX	Migrate to 12.3(4)T or later	
12.2EW		12.2(18)EW
12.2EWA		12.2(20)EWA
12.2JA		12.2(15)JA
12.2JK		12.2(15)JK
12.2MB	Migrate to 12.2(19)SW	
12.2MC	Migrate to 12.3(11)T	
12.2MX	Migrate to 12.3(8)T or later	
12.2SU		12.2(14)SU
12.2SW		12.2(19)SW
12.2SY	Migrate to 12.2(17d)SXB or later	
12.2SZ	Migrate to 12.2(20)S4	
12.2T	12.2(13)T14	
	12.2(15)T7	
12.2XA	Migrate to 12.3 or later	
12.2XB	12.2(2)XB18	
12.2XC	Migrate to 12.3T or later	
12.2XD	Migrate to 12.3 or later	
12.2XE	Migrate to 12.3 or later	
12.2XF	Migrate to 12.2(15)BC2	
12.2XG	Migrate to 12.3 or later	
12.2XH	Migrate to 12.3 or later	
12.2XI	Migrate to 12.3 or later	
12.2XJ	Migrate to 12.3 or later	
12.2XK	Migrate to 12.3 or later	
12.2XL	Migrate to 12.3 or later	
12.2XM	Migrate to 12.3 or later	
12.2XN	Migrate to 12.3 or later	
12.2XQ	Migrate to 12.3 or later	

12.2XR		12.2(15)XR
12.2XS	Migrate to 12.3 or later	
12.2XT	Migrate to 12.3 or later	
12.2XU	Migrate to 12.3 or later	
12.2XV	No plan.	
12.2XW	Migrate to 12.3 or later	
12.2XZ	Migrate to 12.3 or later	
12.2YA	12.2(4)YA8	
12.2YB	Migrate to 12.3 or later	
12.2YC	Migrate to 12.3 or later	
12.2YD	Migrate to 12.3(8)T or later	
12.2YE	Migrate to 12.2(18)S or later	
12.2YF	Migrate to 12.3 or later	
12.2YG	Migrate to 12.3 or later	
12.2YH	Migrate to 12.3 or later	
12.2YJ	Migrate to 12.3 or later	
12.2YL	Migrate to 12.3T or later	
12.2YM	Migrate to 12.3T or later	
12.2YN	Migrate to 12.3T or later	
12.2YO	Migrate to 12.2(17d)SXB or later	
12.2YQ	Migrate to 12.3(4)T or later	
12.2YR	Migrate to 12.3(4)T or later	
12.2YS	Migrate to 12.3T or later	
12.2YU	Migrate to 12.3(2)T or later	
12.2YV	Migrate to 12.3(4)T or later	
12.2YW	Migrate to 12.3(2)T or later	
12.2YX	Migrate to 12.2(14)SU	
12.2YZ	Migrate to 12.2(20)S4	
12.2ZB	Migrate to 12.3T or later	
12.2ZC	Migrate to 12.3T or later	
12.2ZD	Migrate to 12.3 or later	
12.2ZE	Migrate to 12.3 or later	
12.2ZF	Migrate to 12.3(4)T or later	
12.2ZG	Migrate to 12.3(4)T or later	

12.2ZH	Migrate to 12.3(4)T or later	
12.2ZI	Migrate to 12.2(18)S or later	
12.2ZJ	Migrate to 12.3T or later	
12.2ZL	Migrate to 12.3(7)T or later	
12.2ZN	Migrate to 12.3T or later	
12.2ZO	Migrate to 12.3 or later	
12.2ZP	No plan.	
Affected 12.3-Based Release	Rebuild	Maintenance
12.3	12.3(3f)	
		12.3(5)
12.3B		12.3(5a)B4
12.3BC		12.3(9a)BC
12.3BW	Migrate to 12.3(5a)B or later	
12.3T	12.3(2)T5	
	12.3(4)T7	
		12.3(7)T
12.3XA	Migrate to 12.3(7)T or later	
12.3XB	Migrate to 12.3(8)T or later	
12.3XC	Migrate to 12.3(2)XC3 - Availability date TBD	
12.3XD	12.3(4)XD	
12.3XE	12.3(2)XE1	
12.3XF	12.3(2)XF	
12.3XG	12.3(4)XG1	
12.3XH	12.3(4)XH	
12.3XI	12.3(7)XI	
12.3XJ	12.3(7)XJ	
12.3XK	12.3(4)XK1	
12.3XL	12.3(7)XL	
12.3XM	12.3(7)XM	
12.3XN	12.3(4)XN	
12.3XQ	12.3(4)XQ	
12.3XR	12.3(7)XR	

12.3XS	12.3(7)XS
12.3XT	12.3(2)XT
12.3XU	12.3(8)XU
12.3XW	12.3(8)XW
12.3XX	12.3(8)XX
12.3XY	12.3(8)XY
12.3YA	12.3(8)YA
12.3YD	12.3(8)YD
12.3YE	12.3(4)YE
12.3YF	12.3(11)YF
12.3YG	12.3(8)YG
12.3YH	12.3(8)YH

When considering software upgrades, please also consult http://www.cisco.com/en/US/products/products_security_advisories_listing.html and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) for assistance.

Obtaining Fixed Software

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for assistance with the upgrade, which should be free of charge.

Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Please have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

See <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

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.

```
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.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

Status of This Notice: FINAL

THIS ADVISORY IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE ADVISORY OR MATERIALS LINKED FROM THE ADVISORY IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS NOTICE AT ANY TIME.

A stand-alone copy or paraphrase of the text of this security advisory that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- comp.dcom.sys.cisco@newsgate.cisco.com
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

Revision History

Revision 1.1	2005- January- 28	Clarified wording in Summary section. Added version 12.2(15)T7 to Software Versions and Fixes table. Removed versions 12.2S, 12.2SX, 12.2SXA, 12.2SXB and 12.2SXD from the Software Versions and Fixes table.
Revision 1.0	2005- January- 26	Initial public release.

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Optional contact info:

Name:

Email:

Home	How to Buy	Login	Register	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	--------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 1992-2005 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

Updated: Jan 28, 2005

Document ID: 63846
