

Cisco Security Advisory: Cisco Catalyst 6000, 6500 and Cisco 7600 Series MPLS Packet Vulnerability

Advisory ID: cisco-sa-20070228-mpls

<http://www.cisco.com/warp/public/707/cisco-sa-20070228-mpls.shtml>

Revision 1.0

For Public Release 2007 February 28 1600 UTC (GMT)

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

Contents

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

Summary

Cisco Catalyst 6500 series systems that are running certain versions of Cisco Internetwork Operating System (IOS) are vulnerable to an attack from a Multi Protocol Label Switching (MPLS) packet. Only the systems that are running in Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the Multilayer Switch Feature Card (MSFC)) or running with Cisco IOS Software Modularity are affected.

MPLS packets can only be sent from the local network segment.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070228-mpls.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ **Affected Products**

☐ **Vulnerable Products**

The following products are affected by this vulnerability:

- Cisco Catalyst 6500 systems that run 12.2(18)SXF4 with Cisco IOS Software Modularity are affected.

Images that support Cisco IOS Software Modularity have a "-vz" suffix in their image name.

The following is a conclusive list of all image names that are running with Cisco IOS Software Modularity and are affected by this vulnerability.

- s72033-adventerprisek9_wan-vz.122-18.SXF4.bin
- s72033-advipservicesk9_wan-vz.122-18.SXF4.bin
- s72033-entservicesk9_wan-vz.122-18.SXF4.bin
- s72033-ipservices_wan-vz.122-18.SXF4.bin
- s72033-ipservicesk9_wan-vz.122-18.SXF4.bin
- s72033-ipservicesk9-vz.122-18.SXF4.bin

- Cisco Catalyst 6000, 6500 and Cisco 7600 series systems with an MSFC2 or MSFC3 that run in Hybrid Mode are affected.

In Hybrid Mode, Catalyst OS (CatOS) software runs on the Supervisor Engine and IOS runs on the MSFC. It is different from the Native Mode in which IOS runs both on the Supervisor Engine and MSFC.

This vulnerability affects MSFC2, MSFC2a and MSFC3 that run certain images in Hybrid mode.

In Hybrid Mode, IOS images that run on MSFC start with "c6msfc2", "c6msfc2a" or "c6msfc3". Several image names that run on MSFC in hybrid mode are provided below for reference:

- c6msfc2a-adventerprisek9_wan-mz.122-18.SXF
- c6msfc3-jsv-mz.122-14.SX2

☐ **Products Confirmed Not Vulnerable**

These products are not vulnerable:

- Systems that are running in Native Mode without Cisco IOS Software Modularity are not affected.
- Systems without an MSFC2, MSFC2a or MSFC3 are not affected.

No other Cisco products are known to be affected by this vulnerability.

[Top of the section](#) [Close Section](#)

☐ Details

Cisco IOS Software Modularity combines subsystems into individual processes and enhances the Cisco IOS Software memory architecture to provide process-level fault isolation and subsystem "In Service Software Upgrade" (ISSU) capability. These enhancements are delivered in Cisco IOS Software for the Catalyst 6500 Series Supervisor Engine 720 and Supervisor Engine 32. Cisco IOS Software Modularity was first delivered as an option in a Cisco IOS Software Release 12.2(18) SXF4. More information on Modular IOS can be found at the following URL:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd80313e15

Not all 12.2(18)SXF4 images support Modular IOS. Only the images with a "-vz" in the image name support Modular IOS and are affected by this vulnerability. A conclusive list of all affected image names that support Cisco IOS Software Modularity is provided in the Affected Products section.

In Hybrid Mode, a CatOS image is used as the system software to run the Supervisor Engine on the Catalyst systems. If an MSFC is installed, a separate IOS Software image is used in order to run the MSFC. CatOS provides the Layer 2 (L2) switching functionality. The Cisco IOS on the MSFC provides the Layer 3 (L3) routing functionality. It differs from the Native Mode, in which a single Cisco IOS Software image is used as the system software to run both the Supervisor Engine and MSFC on the Catalyst systems. IOS software that runs on MSFC in Hybrid Mode is also affected by this vulnerability. More information about the differences between Hybrid and Native Modes can be found at the following URL:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_white_paper09186a00800c

MPLS packets received by a Route Processor (MSFC) Layer 3 interface can potentially trigger this vulnerability. The system in question does not need to be configured for MPLS to be vulnerable. MPLS packets can only be sent from the local network segment, limiting the scope of the exploitation.

This issue is documented in bug IDs [CSCsd37415](#) ([registered](#) customers only) and [CSCef90002](#) ([registered](#) customers only) .

Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias

parameter when determining the environmental impact of a particular vulnerability.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided an FAQ to answer additional questions regarding CVSS at <http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at <http://intellishield.cisco.com/security/alertmanager/cvss>.

CSCsd37415 - RP crashed on sending MPLS packet to a interface (registered customers only)						
Calculate the environmental score of CSCsd37415 ↗						
CVSS Base Score - 3.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal
CVSS Temporal Score - 2.7						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

CSCef90002 - MSFC crashed due to corrupted program counter (registered customers only)						
Calculate the environmental score of CSCef90002 ↗						
CVSS Base Score - 3.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal
CVSS Temporal Score - 2.7						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

[Top of the section](#) [Close Section](#)

☐ Impact

Successful exploitation of the vulnerability may result in the reload of the system on systems that are running with Cisco IOS Software Modularity and the reload of MSFC on systems that are running in Hybrid Mode.

Repeated exploitation may lead to a denial of service condition.

[Top of the section](#) [Close Section](#)

☐ Software Version and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain that 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") or your contracted maintenance provider for assistance.

Each row of the Cisco IOS software table (below) describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For more information on the terms "Rebuild" and "Maintenance," consult the following URL: <http://www.cisco.com/warp/public/620/1.html>.

Trains	Availability of Fixed Releases	
	Rebuild	Maintenance
12.1E	Not vulnerable	
12.2SXA	Vulnerable. Migrate to 12.2(17d)SXB5 or later	
12.2SXB	12.2(17d)SXB5	
12.2SXD	12.2(18)SXD3	
12.2SXE	Not vulnerable	
12.2SXF (*)	12.2(18)SXF5	

* Only 12.2(18)SXF4 with IOS Software Modularity is affected. 12.2SXF releases that run in Hybrid Mode are not affected. Please see the Affected Products section for more information.

A special patch for 12.2(18)SXF4 with Cisco IOS Software Modularity is also available.

Patch Name: MA0045

Image Name: s72033-AMA0045-patch.122-18.SXF4

The above patch can be downloaded from the Cisco IOS Software Modularity Patch Navigator at <http://tools.cisco.com/swdf/ionpn/jsp/main.jsp>

[Top of the section](#) [Close Section](#)

☐ **Workarounds**

There are no workarounds for this vulnerability.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-amb-20070228-mpls.shtml>

[Top of the section](#) [Close Section](#)

☐ **Obtaining Fixed Software**

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

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>.

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

[Top of the section](#) [Close Section](#)

☐ **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>.

[Top of the section](#) [Close Section](#)

☐ **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 guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix 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 or fix is the most appropriate for use in the intended network before it is deployed.

[Top of the section](#) [Close Section](#)

☐ **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

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.

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ **Exploitation and Public Announcements**

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

This vulnerability was reported by a customer.

[Top of the section](#) [Close Section](#)

☐ **Status of this Notice:FINAL**

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

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

errors.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20070228-mpls.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
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

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.

[Top of the section](#) [Close Section](#)

☐ **Revision History**

Revision 1.0	2007-February-28	Initial public release.
--------------	------------------	-------------------------

[Top of the section](#) [Close Section](#)

☐ **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>.

[Top of the section](#) [Close Section](#)

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)

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

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)