

# Table of Contents

<b><u>Cisco Security Advisory: Cisco 6000/6500/7600 Crafted Layer 2 Frame Vulnerability</u></b> .....	1
<u>Revision 1.0 – FINAL</u> .....	1
<u>For Public Release 2004 February 03 1600 UTC (GMT)</u> .....	1
<u>Please provide your feedback on this document</u> .....	1
<u>Summary</u> .....	1
<u>Affected Products</u> .....	1
<u>Details</u> .....	2
<u>Impact</u> .....	3
<u>Software Versions and Fixes</u> .....	3
<u>Cisco IOS Software</u> .....	3
<u>Cisco CatOS Software</u> .....	4
<u>Obtaining Fixed Software</u> .....	4
<u>Workarounds</u> .....	4
<u>Exploitation and Public Announcements</u> .....	4
<u>Status of This Notice: FINAL</u> .....	4
<u>Distribution</u> .....	5
<u>Revision History</u> .....	5
<u>Cisco Security Procedures</u> .....	5

# Cisco Security Advisory: Cisco 6000/6500/7600 Crafted Layer 2 Frame Vulnerability

## Revision 1.0 – FINAL

For Public Release 2004 February 03 1600 UTC (GMT)

---

Please provide your feedback on this document.

---

**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

A layer 2 frame (as defined in the Open System Interconnection Reference Model) that is encapsulating a layer 3 packet (IP, IPX, etc.) may cause Cisco 6000/6500/7600 series systems with Multilayer Switch Feature Card 2 (MSFC2) that have a FlexWAN or Optical Services Module (OSM) or that run 12.1(8b)E14 to freeze or reset, if the actual length of this frame is inconsistent with the length of the encapsulated layer 3 packet.

This vulnerability may be exploited repeatedly causing a denial of service.

This vulnerability has been addressed by the Cisco Bug IDs CSCdy15598 and CSCeb56052.

There is no workaround available. A software upgrade is needed to address the vulnerability.

This advisory will be posted on the Cisco worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20040203-cat6k.shtml>.

## Affected Products

Cisco 6000/6500/7600 series systems with MSFC2 and a FlexWAN or OSM module are affected.

Cisco 6000/6500/7600 series systems with MSFC2 that are running 12.1(8b)E14 are affected even if they do not have a FlexWAN or OSM module.

Cisco 6000/6500/7600 series systems with a Supervisor 720 are not affected by this vulnerability.

The affected systems may be running native or hybrid code.

The **show module** command can be used to determine if there is a FlexWAN or OSM module on the system. A FlexWAN module will have the part number WS-X6182-2PA. The OSM modules will have OSM in the part number.

Refer to <http://www.cisco.com/warp/customer/473/96.html> for more information about determining the type of the MSFC used on the system.

This vulnerability only affects Cisco 6000/6500/7600 series systems with the specified hardware or software configuration. All other systems are not affected by this vulnerability even though they may run affected versions of IOS.

To determine the software running on a Cisco product, log in to the device and issue the show version command to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS®". On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the IOS release name. Other Cisco devices will not have the show version command or will give different output.

The following example identifies a Cisco product running IOS release 12.1(11b)E1 with an installed image name of C6MSFC2-JSV-M:

```
Cisco Internetwork Operating System Software IOS (tm)
```

```
MSFC2 Software (C6MSFC2-JSV-M), Version 12.1(11b)E1, EARLY DEPLOYMENT RELEASE  
SOFTWARE (fc1)
```

## Details

A layer 2 frame that is encapsulating a protocol independent layer 3 packet (IP, IPX, etc.) may cause Cisco 6000/6500/7600 series systems with an MSFC2 to freeze or reset. The actual length of the layer 2 frame needs to be inconsistent with the length of the encapsulated layer 3 packet.

A layer 3 packet that is routed by the Cisco 6000/6500/7600 series systems may trigger this vulnerability if the packet is encapsulated in a specifically crafted layer 2 frame. Crafted packets must be software switched on the vulnerable systems to trigger this vulnerability. The packets that are switched in hardware will not trigger this vulnerability.

Although such frames can only be sent from the local network segment, there might be some cases where it is possible to trigger this vulnerability remotely. For remote exploitation, the crafted layer 2 frames need to pass through all the intermediate layer 3 devices between the source and the destination without being clipped. Remote exploitation will not be possible even if only a single layer 3 device on the path from source to destination clips the crafted layer 2 frame. To the best of our knowledge, only Cisco 6000/ 6500/7600 series will forward such crafted frames without being corrected.

This vulnerability has been addressed by the Cisco Bug IDs CSCdy15598 and CSCeb56052.

- **CSCdy15598** Affects Cisco 6000/6500/7600 series with an MSFC2 and a FlexWAN or OSM module. The systems that do not have a FlexWAN or OSM will not be affected by this bug.
- **CSCeb56052** Affects Cisco 6000/6500/7600 series with an MSFC2 module. Only 12.1(8b)E14 is affected by this bug, other software versions are not affected. The systems without a FlexWAN or OSM will still be affected by this bug if they are running 12.1(8b)E14.

You can use the Bug Toolkit ( registered customers only) to look up the details of these bugs.

Cisco Security Advisory: Cisco 6000/6500/7600 Crafted Layer 2 Frame Vulnerability

# Impact

The exploitation of this vulnerability can result in freeze or the reset of the system. A system that is frozen due to this vulnerability can be recovered by a system reset.

Repeated exploitation may lead to a denial of service until a fixed version of software has been loaded.

## Software Versions and Fixes

### Cisco IOS Software

Each row of the 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 and the anticipated date of availability for each are listed in the Rebuild, Interim, and Maintenance columns. A device running any release in the given train that is earlier than the release in a specific column (less than the earliest fixed release) is known to be vulnerable, and it should be upgraded at least to the indicated release or a later version (greater than the earliest fixed release label).

When selecting a release, keep in mind the following definitions:

- **Rebuild** Constructed from the previous maintenance or major release in the same train, it contains the fix for a specific vulnerability. Although it receives less testing, it contains only the minimal changes necessary to effect the repair. Cisco has made available several rebuilds of mainline trains to address this vulnerability, but strongly recommends running only the latest maintenance release on mainline trains.
- **Interim** Built at regular intervals between maintenance releases and receives less testing. Interims should be selected only if there is no other suitable release that addresses the vulnerability, and interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available through manufacturing, and usually they are not available for customer download from CCO without prior arrangement with the Cisco Technical Assistance Center (TAC).
- **Maintenance** Most heavily tested and highly recommended release of any label in a given row of the table.

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 TAC for assistance, as shown in the section following this table.

Trains	Availability of Fixed Releases		
	Rebuild	Interim	Maintenance
12.1E	12.1(8b)E15	12.1(13.5)E	12.1(19)E
	12.1(11b)E14		
	12.1(13)E1		
12.2SY			12.2(14)SY
12.2ZA			12.2(14)ZA

## Cisco CatOS Software

Cisco CatOS is not affected by this vulnerability. In the case of hybrid code, there is no need to change the Cisco CatOS software version.

## Obtaining Fixed Software

Customers with contracts should obtain upgraded software free of charge through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on the Cisco worldwide website at <http://www.cisco.com/tacpage/sw-center/sw-ios.shtml>.

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 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](mailto: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. To ensure prompt service by email or by phone, please provide your name, company name, address, product serial number, and current version of Cisco IOS software that you are using. This can be documented by pasting the output of the show version command into the text of an email. Free upgrades for non-contract customers must be requested through the TAC.

Please do not contact either "[psirt@cisco.com](mailto:psirt@cisco.com)" or "[security-alert@cisco.com](mailto: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, instructions, and e-mail addresses for use in various languages.

## Workarounds

There is no workaround available. The vulnerability can not be mitigated by reconfiguring the affected systems. A software upgrade is needed.

## 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 is a final advisory. Although Cisco cannot guarantee the accuracy of all statements in this advisory, all of the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of

this advisory unless there is some material change in the facts. Should there be a significant change in the facts, Cisco will update this advisory.

A standalone 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-20040203-cat6k.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](mailto:cust-security-announce@cisco.com)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- 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 1.0	2004-February-03	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/warp/public/707/sec\\_incident\\_response.shtml](http://www.cisco.com/warp/public/707/sec_incident_response.shtml). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

---

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.