

# Cisco Security Advisory: OSM Line Card Header Corruption Vulnerability

Document ID: 29403

Advisory ID: cisco-sa-20021211-osm-lc-ios

<http://www.cisco.com/warp/public/707/cisco-sa-20021211-osm-lc-ios.shtml>

## Revision 1.0

For Public Release 2002 December 11 1600 UTC (GMT)

---

Please provide your feedback on this document.

---

**Summary**  
**Affected Products**  
**Details**  
**Impact**  
**Software Versions and Fixes**  
**Workarounds**  
**Obtaining Fixed Software**  
**Exploitation and Public Announcements**  
**Status of This Notice: FINAL**  
**Distribution**  
**Revision History**  
**Cisco Security Procedures**

---

## Summary

The Optical Service Module (OSM) Line Cards installed in Catalyst 6500 or Cisco 7600 chassis, and running Cisco IOS® Software Version 12.1(8)E and higher are vulnerable to a Denial of Service upon receiving a specifically constructed or corrupted packet from the local network.

Cisco has provided fixed software for this problem. The vulnerability has been assigned Cisco Bug ID CSCdy29717.

The complete advisory will be available at  
<http://www.cisco.com/warp/public/707/cisco-sa-20021211-osm-lc-ios.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

The following products are affected only when they have OSM Line Cards installed and running in conjunction with Cisco IOS Software Versions 12.1(8)E through 12.1(13.4)E:

- Catalyst 6500 with Sup2/MSFC2 modules
- Cisco 7600

## Products Confirmed Not Vulnerable

No other releases of Cisco Catalyst hardware and software combinations are affected by this vulnerability. No other Cisco products are affected by this vulnerability.

## Details

This defect was introduced by CSCdv23236 in version Cisco IOS Software Versions 12.1(8)E. When certain malformed datagrams arrive on the interface, the packet forwarding engine specific to this line card rewrites the datagram in such a way that legitimate information is overwritten resulting in the interface ceasing to receive and forward further legitimate network traffic.

Because most networking devices typically drop the malformed datagrams, the attack must occur from a locally attached network.

### Bug ID

- CSCdy29717 – Traffic forwarding stops due to packet header corruption.

## Impact

This defect causes traffic forwarding to fail, resulting in a denial of service. This can only be triggered from the local network and is not propagated across networks by most layer 3 devices.

## Software Versions and Fixes

This vulnerability is repaired in version 12.1(13.5)E, and is available for general download in version 12.1(13)E1 and 12.1(12c)E2, and will be available going forward in all versions supporting this hardware combination, specifically 12.1(14)E. The 12.2S train is not affected by this vulnerability, as this particular hardware combination is not currently supported with the 12.2S software.

## Workarounds

No workarounds exist for this vulnerability. Cisco recommends upgrading to repaired versions.

## Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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.

## 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 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.

## 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](mailto: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/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.

## 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 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.

## Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20021211-osm-lc-ios.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 web. Users concerned about this problem are encouraged to check the URL given above for any updates.

## Revision History

Revision 1.0	2002-December-11	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](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>.

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Dec 11, 2002

Document ID: 29403

---