

Cisco Security Advisory: Cisco ONS Platform Crafted Packet Vulnerability

Advisory ID: cisco-sa-20090114-ons

<http://www.cisco.com/warp/public/707/cisco-sa-20090114-ons.shtml>

Revision 1.1

Last Updated 2009 January 16 1300 UTC (GMT)

For Public Release 2009 January 14 1600 UTC (GMT)

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

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring 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 Cisco ONS 15300 series Edge Optical Transport Platform, the Cisco ONS 15454 Optical Transport Platform, the Cisco ONS 15454 SDH Multiservice Platform, and the Cisco ONS 15600 Multiservice Switching Platform contains a vulnerability when processing TCP traffic streams that may result in a reload of the device control card.

Cisco has released free software updates that address this vulnerability.

There are no workarounds that mitigate this vulnerability. Several mitigations exist that can limit the exposure of this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090114-ons.shtml>.

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

☐ Affected Products

☐ Vulnerable Products

The following Cisco ONS products are vulnerable if running affected software versions:

- Cisco ONS 15310-CL and 15310-MA
- Cisco ONS 15327
- Cisco ONS 15454 and 15454 SDH
- Cisco ONS 15600

Consult the section "Software Versions and Fixes" within this advisory for affected software versions. To determine your software version, view the **Help > About window** on the CTC management software).

☐ Products Confirmed Not Vulnerable

The following Cisco ONS products are confirmed not vulnerable:

- Cisco ONS 15800 Series

- Cisco ONS 15500 Series Extended Service Platform
- Cisco ONS 15302
- Cisco ONS 15305
- Cisco ONS 15200 Series Metro DWDM Systems
- Cisco ONS 15190 Series IP Transport Concentrator

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

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

☐ Details

The affected Cisco 15310-CL, 15310-MA, ONS 15327, ONS 15454, ONS 15454 SDH, and ONS 15600 hardware is managed through the CTX, CTX2500, XTC, TCC/TCC+/TCC2/TCC2P, TCCi/TCC2/TCC2P, and TSC control cards respectively. These control cards are usually connected to a Data Communications Network (DCN). In this context the term DCN is used to denote the network that transports management information between a management station and the network entity (NE). This definition of DCN is sometimes referred to as Management Communication Network (MCN). The DCN is usually physically or logically separated from the optical data network and isolated from the Internet. This limits the exposure to the exploitation of this vulnerability from the Internet.

A crafted stream of TCP traffic to the control cards on a node will result in a reset of the corresponding control cards on this node. A complete 3-way handshake is required on any open TCP port to be able to exploit this vulnerability.

The timing for the data channels traversing the switch is provided by the control cards.

When an active and a standby Cisco ONS 15310-MA, ONS 15310-CL, ONS 15327, ONS 15454 or ONS 15454 SDH control card reloads at the same time, the synchronous data channels traversing the switch drop traffic until the card comes back online. Asynchronous data channels traversing the switch are not impacted. Manageability functions provided by the network element using the CTX, CTX2500, XTC or TCC/TCC+/TCC2/TCC2P control cards are not available until the control card comes back online.

On the Cisco ONS 15600 hardware, whenever both the active and standby control cards are rebooting at the same time, there is no impact to the data channels traversing the switch because the TSC performs a software reset which does not impact the timing being provided by the TSC for the data channels.

Manageability functions provided by the network element through the TSC control cards are not available until the control card comes back online.

This vulnerability is documented in Cisco bug ID [CSCsr41128](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-3818.

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

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

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

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

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>.

CSCsr41128: Cisco ONS Crafted TCP Packet Vulnerability					
Calculate the environmental score of CSCsr41128					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					
Exploitability	Remediation Level			Report Confidence	

Functional	Official-Fix	Confirmed
------------	--------------	-----------

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

[-] Impact

Successful exploitation of this vulnerability will result in a reset of the node's control card. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition, dropping the synchronous data channels traversing the switch (Cisco ONS 15310-MA, ONS 15310-CL, ONS 15327, ONS 15454, ONS 15454 SDH) and preventing manageability functions provided by the network element control cards (all ONS switches) until the control card comes back online.

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

[-] Software Versions 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 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.

Affected Major Release	Affected Releases	First Fixed Release
6.x and earlier	Not Vulnerable.	
7.0	7.0.2, 7.0.4, 7.0.5	7.0.7
7.2	7.2.0, 7.2.2	7.2.3
8.0	Vulnerable; migrate to 8.5.3 or later.	
8.5	8.5.0, 8.5.1, 8.5.2	8.5.3
9.0	Not Vulnerable.	

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

Workarounds

There are no workarounds for this vulnerability. The following general mitigation actions help prevent remote exploitation:

- Isolate DCN:
Ensuring the DCN is physically or logically separated from the customer network and isolated from the Internet will limit the exposure to the exploitation of these vulnerabilities from the Internet or customer networks.
- Apply Transit Access Control Lists:
Apply access control lists (ACLs) on routers / switches / firewalls installed in front of the vulnerable network devices such that TCP/IP traffic destined for the CTX, CTX2500, XTC, TCC2/TCC2+/TCC2P, or TSC control cards on the ONS is allowed only from the network management workstations.
For examples on how to apply ACLs on Cisco routers, refer to the white paper "Transit Access Control Lists: Filtering at Your Edge", which is available at the following link: http://www.cisco.com/en/US/customer/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml.

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, which is available at the following link: <http://www.cisco.com/warp/public/707/cisco-amb-20090114-ons.shtml>.

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

Obtaining Fixed Software

Cisco has released free software updates that address these vulnerabilities. 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/en/US/docs/general/warranty/English/EU1KEN.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of 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 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.

This vulnerability was found by reviewing Cisco TAC service requests.

[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-20090114-ons.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-bulletins@lists.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 1.1	2009-January-16	Replaced software table.
Revision 1.0	2009-January-14	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.](#)