

Cisco Security Advisory: Cisco ONS15454 IP TOS Bit Vulnerability

Document ID: 24621

Advisory ID: cisco-sa-20020619-ons-tos

<http://www.cisco.com/warp/public/707/cisco-sa-20020619-ons-tos.shtml>

Revision 1.0

For Public Release 2002 June 19 1500 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 Advisory: FINAL
- Distribution
- Revision History
- Cisco Security Procedures

Summary

The Cisco ONS15454 optical transport platform is vulnerable when IP packets, with the Type Of Service (TOS) bit set, are sent to the Timing Control Card (TCC) LAN interface. Cisco ONS software releases 3.1.0 to 3.2.0, both inclusive, are vulnerable.

This vulnerability is documented as Cisco bug ID CSCdx48853. There are workarounds available to mitigate the effects of this vulnerability.

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20020619-ons-tos.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

All Cisco ONS15454 hardware running Cisco ONS release 3.1.0 to 3.2.0, both inclusive, is affected by this vulnerability.

To determine your software revision, view the help—about window on the CTC.

Products Confirmed Not Vulnerable

Hardware not affected includes the Cisco ONS15327 edge optical transport platform, Cisco ONS15540 extended service platform, ONS15800 series, ONS15200 series metro DWDM systems and the ONS15194 IP transport concentrator.

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

When an IP packet with non-zero TOS bits in its header is received by the TCC on its LAN interface, this causes software versions 3.1.0 and later to reset the TCC. When the crafted packets are sent repeatedly, both TCCs reset leaving no active TCC in the platform.

In order to exploit this vulnerability, an attacker must be able to establish an IP connection to the TCC's LAN interface.

This vulnerability is documented as Cisco bug ID CSCdx48853, which requires a CCO account to view, and can be viewed after 2002 June 20 at 1500 UTC.

Impact

When both TCCs are reset simultaneously, the E100 cards and E1000 cards stop passing traffic. The G1000 cards traffic would not be affected. TDM traffic may be compromised because timing is not synchronized anymore. The protection switching feature is compromised.

Software Versions and Fixes

This vulnerability is fixed in Cisco ONS software release 3.2.1 and later.

Cisco ONS software release 3.2.1 is the maintenance release fix version for this vulnerability. Cisco ONS software version 3.3.0 is currently available as an interim fix release for this vulnerability until Cisco ONS software version 3.2.1 is released at the end of July 2002.

The procedure to upgrade to the fixed software version on the Cisco ONS 15454 is detailed at: <http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/r33docs/sftuprgd/index.htm>.

Workarounds

Restrict IP traffic to the gateway node(s) with a router configured to change the TOS to zero for all out-bound packets going to the TCC.

Sample Cisco router configuration:

```
class-map match-all MY_LAN
  match any

!--- Matches all packets
```

```
!
!
policy-map SET_TOS
class MY_LAN
set ip dscp default

!--- Sets all packets to "00000000" (Best effort)

!
interface FastEthernet0/0
service-policy output SET_TOS

!--- Modifies outbound packets
```

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

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

This defect was reported by a Cisco customer. The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory..

Status of This Advisory: 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-20020619-ons-tos.shtml>.

In addition to worldwide website posting, a text version of this advisory is clear-signed with the Cisco PSIRT PGP keyID 0x1A88BFC5 with fingerprint 17E6 4AC4 4DD5 F889 1560 919D 3FC6 EA52 1A88 BFC5 and is posted to the following e-mail and Usenet news recipients:

- cust-security-announce@cisco.com
- bugtraq@securityfocus.com
- firewalls@lists.gnac.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- 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	2002-Jun-19	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/go/psirt>. This includes instructions for press inquiries regarding Cisco security advisories.

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

Updated: Jun 19, 2002

Document ID: 24621
