

Table of Contents

<u>Cisco Security Advisory: Cisco ONS 15327, ONS 15454, ONS 15454 SDH, and ONS 15600</u>	
<u>Vulnerabilities</u>	1
<u>Revision 1.0</u>	1
<u>For Public Release 2004 February 19 1700 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>	4
<u>Obtaining Fixed Software</u>	5
<u>Workarounds</u>	5
<u>Exploitation and Public Announcements</u>	6
<u>Status of This Notice: FINAL</u>	6
<u>Distribution</u>	6
<u>Revision History</u>	7
<u>Cisco Security Procedures</u>	7

Cisco Security Advisory: Cisco ONS 15327, ONS 15454, ONS 15454 SDH, and ONS 15600 Vulnerabilities

Revision 1.0

For Public Release 2004 February 19 1700 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

Multiple vulnerabilities exist in the Cisco ONS 15327 Edge Optical Transport Platform, the Cisco ONS 15454 Optical Transport Platform, the Cisco ONS 15454 SDH Multiplexer Platform, and the Cisco ONS 15600 Multiservice Switching Platform.

These vulnerabilities are documented as Cisco bug ID CSCec17308/CSCec19124(tftp), CSCec17406(port 1080), and CSCec66884/CSCec71157(SU access). There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20040219-ONS.shtml>.

Affected Products

- CSCec17308/CSCec19124(tftp)

Product	Affected Releases
15327	4.1(0) to 4.1(2) 4.0(x)
15454, 15454 SDH	4.5(x) 4.1(0) to 4.1(2)

	4.0(x)
15600	1.0(x)

- **CSCec17406(port 1080)**

Product	Affected Releases
15327	4.1(0) 4.0(0) to 4.0(1)
15454, 15454 SDH	4.5(x) 4.1(0) 4.0(0) to 4.0(1)
15600	Not Affected

- **CSCec66884/CSCec71157(SU access)**

Product	Affected Releases
15327	4.1(0) to 4.1(2) 4.0(x)
15454, 15454 SDH	4.5(x) 4.1(0) to 4.1(2) 4.0(x)
15600	1.x(x) except for 1.1(1)

Products not affected by these vulnerabilities include the Cisco ONS 15800 series, ONS 15500 series extended service platform, ONS 15302, ONS 15305, ONS 15200 series metro DWDM systems, and the ONS 15190 series IP transport concentrator.

Cisco ONS 15327 hardware running ONS Release 1.x(x) and 3.x(x) and Cisco ONS 15454 hardware running ONS Releases 2.x(x) and 3.x(x) are not affected by these vulnerabilities.

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

To determine your software revision, view the **Help > About** window on the CTC management software.

Details

The affected Cisco ONS 15327, ONS 15454, ONS 15454 SDH, and ONS 15600 hardware is managed through the XTC, TCC+/TCC2, TCCi/TCC2, and TSC control cards respectively. These control cards are usually connected to a network isolated from the Internet and local to the customer's environment. This limits the exposure to the exploitation of the vulnerabilities from the Internet.

- **CSCec17308/CSCec19124(tftp)**

The TFTP service on UDP port 69 is enabled by default to allow both **GET** and **PUT** commands to be executed without any authentication. Using a TFTP client, it is possible to connect to the optical device and upload or retrieve ONS system files on the current active TCC in the /flash0 or /flash1 directories. It is not possible to upload or retrieve any user data files.

Cisco bug ID CSCec17308 documents the issue on the Cisco ONS 15327, ONS 15454 and ONS 15454 SDH, and Cisco bug ID CSCec19124 documents the issue on the Cisco ONS 15600 hardware.

- **CSCec17406(port 1080)**

The Cisco ONS 15327, ONS 15454 and ONS 15454 SDH hardware is susceptible to an ACK Denial of Service (DoS) attack on TCP port 1080. TCP port 1080 is used by network management applications to communicate with the controller card. The controller card on the optical device will reset under such an attack.

An ACK DoS attack is conducted by not sending the final ACK required for a 3-way TCP handshake to complete, and instead sending an invalid response to move the connection to an invalid TCP state.

The Cisco ONS 15600 Multiservice Switching Platform is not affected by this vulnerability.

- **CSCec66884/CSCec71157(SU access)**

Telnet access to the underlying VxWorks operating system, by default, is restricted to Superusers only. Due to this vulnerability, a superuser whose account is locked out, disabled, or suspended is still able to login (Telnet) into the VxWorks shell, using their previously configured password.

Cisco bug ID CSCec66884 documents the issue on the Cisco ONS 15327, ONS 15454 and ONS 15454 SDH, and Cisco bug ID CSCec71157 documents the issue on the Cisco ONS 15600 hardware.

The Internetworking Terms and Cisco Systems Acronyms online guides can be found at <http://www.cisco.com/univercd/cc/td/doc/cisintwk/>.

These vulnerabilities are documented in the Cisco Bug Toolkit (registered customers only) as Cisco bug IDs CSCec17308/CSCec19124(tftp), CSCec17406(port 1080), and CSCec66884/CSCec71157(SU access). To access this tool, you must be a registered user and you must be logged in.

Impact

- **CSCec17308/CSCec19124(tftp)** — This vulnerability could be exploited to launch a DoS attack on the optical device if corrupt ONS system files were to be uploaded to the controller card.
- **CSCec17406(port 1080)** — This vulnerability could be exploited to launch a DoS attack on the optical device.

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

On the Cisco ONS 15454, ONS 15327, and ONS 15454 SDH hardware, whenever both the active and standby control cards are rebooting at the same time, the synchronous data channels traversing the switch drop traffic until the card reboots. Asynchronous data channels traversing the switch are not impacted. Manageability functions provided by the network element using the TCC+/TCC2, XTC, and TCCi/TCC2 control cards are not available until the control card reboots.

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 does 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 reboots.

- **CSCec66884/CSCec71157(SU access)** — This vulnerability could be exploited to gain unauthorized access to the optical device.

Software Versions and Fixes

- **CSCec17308/CSCec19124(tftp)**

Product	Fixed Releases
15327	4.1(3) and later
15454, 15454 SDH	4.6(1) and later, 4.1(3) and later
15600	1.3(0) and later, 1.1(0) and later

- **CSCec17406(port 1080)**

Product	Fixed Releases
15327	4.1(1) and later, 4.0(2) and later
15454, 15454 SDH	4.6(1) and later, 4.1(1) and later, 4.0(2) and later
15600	Not Affected

- **CSCec66884/CSCec71157(SU access)**

Product	Fixed Releases
15327	4.1(3) and later
15454, 15454 SDH	4.6(1) and later, 4.1(3) and later
15600	1.1(1), 5.0 and later (when available)

Cisco ONS Release 4.6(0) is not affected by these vulnerabilities. The recommended release to upgrade to is Cisco ONS release 4.6(1).

Upgrade procedures can be found as indicated below.

- The procedure to upgrade to the fixed software version on the Cisco ONS 15327 hardware is detailed at <http://www.cisco.com/univercd/cc/td/doc/product/ong/15327/327doc41/index.htm>.
- The procedure to upgrade to the fixed software version on the Cisco ONS 15454 hardware is detailed at <http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/r46docs/index.htm>.
- The procedure to upgrade to the fixed software version on the Cisco ONS 15600 hardware is detailed at <http://cisco.com/univercd/cc/td/doc/product/ong/15600/index.htm>.

Obtaining Fixed Software

Cisco is offering free software upgrades to address this vulnerability for all affected customers.

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 the Cisco Connection Online Software Center at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

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/tacpage/sw-center/sw-optical.shtml>. To access the software download URL, you must be a registered user and you must be logged in.

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 obtaining the software upgrade(s).

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) using the contact information listed below. In these cases, customers are entitled to obtain an upgrade to a later version of the same release or as indicated by the applicable corrected software version in the Software Versions and Fixes section (noted above).

Cisco 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

See <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.

Please have your product serial number available and give the URL of this notice as evidence of your entitlement to an upgrade. Upgrades for non-contract customers must be requested through the TAC.

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

Workarounds

There are mitigation workarounds available for these vulnerabilities. The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code.

- **CSCec17308/CSCec19124(tftp)**

Use access control lists on routers and firewalls that are installed in the network to allow only valid network management workstations to gain TFTP access to the XTC, TCC+/TCC2, TCCi/TCC2, or TSC control cards.

- **CSCec17406(port 1080)**

Use access control lists on routers and firewalls that are installed in the network to allow only valid network management workstations to gain TCP port 1080 access to the XTC, TCC+/TCC2, TCCi/TCC2, or TSC control cards.

- **CSCec66884/CSCec71157(SU access)**

Use access control lists on routers and firewalls that are installed in the network to allow only valid network management workstations to gain login (Telnet) access to the XTC, TCC+/TCC2, TCCi/TCC2, or TSC control cards.

Refer to <http://www.cisco.com/warp/public/707/iacl.html> for examples on how to apply access control lists (ACLs) on Cisco routers.

Exploitation and Public Announcements

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

These vulnerabilities were reported to PSIRT by Cisco customers or found during internal testing.

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 may update this advisory.

A stand-alone 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-20040219-ONS.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key having the fingerprint 8C82 5207 0CA9 ED40 1DD2 EE2A 7B31 A8CF 32B6 B590 and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- comp.dcom.sys.cisco@newsgate.cisco.com
- 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-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/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>.

This advisory is copyright 2004 by Cisco Systems, Inc. This advisory may be redistributed freely after the release date given at the top of the text, provided that redistributed copies are complete and unmodified, including all date and version information.

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