

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

## Revision 1.0

For Public Release 2004 July 21 at 1600 UTC (GMT)

---

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

---

## Contents

[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

Cisco has fixed multiple malformed packet vulnerabilities in the TCP/IP stacks of 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 the following Cisco bug IDs

- CSCed06531 (IP)
- CSCed86946 (ICMP)
- CSCec88426/CSCec88508/CSCed85088/CSCeb07263/CSCec21429 (TCP)
- CSCec59739/CSCed02439/CSCed22547 (Last-ACK)
- CSCec88402/CSCed31918/CSCed83309/CSCec85982/CSCec21435/CSCee03697 (UDP)
- CSCea16455/CSCea37089/CSCea37185 (SNMP)
- CSCee27329 (passwd)

There are workarounds available to mitigate the exposure to these vulnerabilities in the workaround section of this advisory. Cisco is providing fixed software, and recommends that customers upgrade to it.

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20040721-ons.shtml>.

## Affected Products

### Vulnerable Products

- CSCed06531 (IP)

Product	Affected Releases
15327	4.6(0) and 4.6(1) 4.1(0) to 4.1(3) 4.0(0) to 4.0(2) 3.x(x) and earlier
15454, 15454 SDH	4.6(0) and 4.6(1) 4.5(x) 4.1(0) to 4.1(3) 4.0(0) to 4.0(2) 3.x(x) earlier than 2.3(5)
15600	Not Affected

- CSCed86946 (ICMP)

Product	Affected Releases
---------	-------------------

15327	4.6(0) and 4.6(1) 4.1(0) to 4.1(3) 4.0(0) to 4.0(2) 3.x(x) and earlier
15454, 15454 SDH	4.6(0) and 4.6(1) 4.5(x) 4.1(0) to 4.1(3) 4.0(0) to 4.0(2) 3.x(x) earlier than 2.3(5)
15600	Not Affected

● **CSCec88426/CSCec88508/CSCed85088/CSCeb07263/CSCec21429 (TCP)**

Product	Affected Releases
15327	4.6(0) and 4.6(1) 4.1(0) to 4.1(3) 4.0(0) to 4.0(2) 3.x(x) and earlier
15454, 15454 SDH	4.6(0) and 4.6(1) 4.5(x) 4.1(0) to 4.1(3) 4.0(0) to 4.0(2) 3.x(x) earlier than 2.3(5)
15600	1.x(x)

● **CSCec59739/CSCed02439/CSCed22547 (Last-ACK)**

Product	Affected Releases
15327	4.6(0) and 4.6(1) 4.1(0) to 4.1(3) 4.0(0) to 4.0(2) 3.x(x) and earlier
15454, 15454 SDH	4.6(0) and 4.6(1) 4.5(x) 4.1(0) to 4.1(3) 4.0(0) to 4.0(2) 3.x(x) earlier than 2.3(5)
15600	Not Affected

- **CSCec88402/CSCed31918/CSCed83309/CSCec85982/CSCec21435/CSCee03697 (UDP)**

Product	Affected Releases
15327	4.6(0) and 4.6(1) 4.1(0) to 4.1(3) 4.0(0) to 4.0(2) 3.x(x) and earlier
15454, 15454 SDH	4.6(0) and 4.6(1) 4.5(x) 4.1(0) to 4.1(3) 4.0(0) to 4.0(2) 3.x(x) earlier than 2.3(5)
15600	1.x(x)

- **CSCea16455/CSCea37089/CSCea37185 (SNMP)**

Product	Affected Releases
15327	4.1(0) to 4.1(2) 4.0(0) to 4.0(2) 3.x(x) and earlier
15454, 15454 SDH	4.5(x) 4.1(0) to 4.1(2) 4.0(0) to 4.0(2) 3.x(x) earlier than 2.3(5)
15600	Not Affected

- **CSCee27329 (passwd)**

Product	Affected Releases
15327	4.6(0) and 4.6(1)
15454, 15454 SDH	4.6(0) and 4.6(1)
15600	Not Affected

## Products Confirmed Not Vulnerable

For clarification, the following products are not affected by these vulnerabilities.

- Cisco ONS 15800 series
- ONS 15500 series extended service platform
- ONS 15302, ONS 15305, ONS 15200 series metro DWDM systems

- ONS 15190 series IP transport concentrator

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/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.

- **CSCed06531 (IP)**

Malformed IP packets may potentially cause the XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to be resetting at the same time.

The Cisco ONS 15600 hardware is not affected by this issue.

- **CSCed86946 (ICMP)**

Malformed ICMP packets may potentially cause the XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to be resetting at the same time.

The Cisco ONS 15600 hardware is not affected by this issue.

- **CSCec88426/CSCec88508/CSCed85088/CSCeb07263/CSCec21429 (TCP)**

Malformed TCP packets may potentially cause the XTC, TCC/TCC+/TCC2, TCCi/TCC2 and TSC control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to be resetting at the same time.

Cisco bug IDs CSCec88426, CSCec88508, and CSCed85088 document the issue on the Cisco ONS 15327, ONS 15454 and ONS 15454 SDH, and Cisco bug IDs CSCeb07263 and CSCec21429 documents the issue on the Cisco ONS 15600 hardware.

There is no traffic impact on the Cisco ONS 15600 hardware; only manageability functions are affected because of this issue.

- **CSCec59739/CSCed02439/CSCed22547 (Last-ACK)**

The XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards are susceptible to a TCP-ACK Denial of Service (DoS) attack on open TCP ports. The controller card on the optical device will reset under such an attack.

A TCP-ACK DoS attack is conducted by not sending the regular 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 hardware is not affected by this issue.

- **CSCec88402/CSCed31918/CSCed83309/CSCec85982/CSCec21435/CSCee03697 (UDP)**

Malformed UDP packets may potentially cause the XTC, TCC/TCC+/TCC2, TCCi/TCC2 and TSC control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to be resetting at the same time.

Cisco bug IDs CSCec88402, CSCed31918, CSCed83309, and CSCec85982 document the issue on

the Cisco ONS 15327, ONS 15454 and ONS 15454 SDH, and Cisco bug ID CSCec21435 and CSCee03697 document the issue on the Cisco ONS 15600 hardware.

There is no traffic impact on the Cisco ONS 15600 hardware; only manageability functions are affected because of this issue.

- **CSCea16455/CSCea37089/CSCea37185 (SNMP)**

Malformed SNMP packets may potentially cause the XTC, TCC/TCC+/TCC2 and TCCi/TCC2 control cards to reset. Repeated transmission of these malformed packets could cause both the control cards to be resetting at the same time.

The Cisco ONS 15600 hardware is not affected by this issue.

- **CSCee27329 (passwd)**

If an account has a blank password set, and an attempt was made to log into the device with a password greater than ten characters the attempt would be successful.

This vulnerability only affects the TL1 login interface. The CTC login interface is not vulnerable to this vulnerability.

The CTC and TL1 user interfaces prevent the setting of a blank password as the password. Only the CISCO15 userid, during initial install process has a blank password which is to be changed as part of the initial install process.

The Cisco ONS 15600 hardware is not affected by this issue.

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 as Bug IDs

[CSCed06531 \(IP\)](#),

[CSCed86946 \(ICMP\)](#),

[CSCec88426/CSCec88508/CSCed85088/CSCeb07263/CSCec21429 \(TCP\)](#),

[CSCec59739/CSCed02439/CSCed22547 \(Last-ACK\)](#),

[CSCec88402/CSCed31918/CSCed83309/CSCec85982/CSCec21435/CSCee03697 \(UDP\)](#),

[CSCea16455/CSCea37089/CSCea37185 \(SNMP\)](#), and

[CSCee27329 \(passwd\)](#) ( [registered](#) customers only) .

## Impact

The malformed packet vulnerabilities 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.

The CSCee27329 (passwd) vulnerability could be exploited to gain unauthorized access to an account with a blank password set.

## Software Versions and Fixes

First fixed software release table for all vulnerabilities referenced in this Security Advisory

Product	Fixed Releases
15327	4.6(2) and later 4.1(4) and later 4.0(3) and later
15454, 15454 SDH	4.6(2) and later 4.1(4) and later 4.0(3) and later 2.3(5)
15600	5.0 and later

- **CSCed06531 (IP)**

Product	Fixed Releases
15327	4.6(2) and later 4.1(4) and later 4.0(3) and later
15454, 15454 SDH	4.6(2) and later 4.1(4) and later 4.0(3) and later 2.3(5)
15600	Not Affected

- **CSCed86946 (ICMP)**

Product	Fixed Releases
---------	----------------

15327	4.6(2) and later 4.1(4) and later 4.0(3) and later
15454, 15454 SDH	4.6(2) and later 4.1(4) and later 4.0(3) and later 2.3(5)
15600	Not Affected

● CSCec88426/CSCec88508/CSCed85088/CSCeb07263/CSCec21429 (TCP)

Product	Fixed Releases
15327	4.6(2) and later 4.1(4) and later 4.0(3) and later
15454, 15454 SDH	4.6(2) and later 4.1(4) and later 4.0(3) and later 2.3(5)
15600	5.0 and later

● CSCec59739/CSCed02439/CSCed22547 (Last-ACK)

Product	Fixed Releases
15327	4.6(2) and later 4.1(4) and later 4.0(3) and later
15454, 15454 SDH	4.6(2) and later 4.1(4) and later 4.0(3) and later 2.3(5)
15600	Not Affected

● CSCec88402/CSCed31918/CSCed83309/CSCec85982/CSCec21435/CSCee03697 (UDP)

Product	Fixed Releases
15327	4.6(2) and later 4.1(4) and later 4.0(3) and later

15454, 15454 SDH	4.6(2) and later 4.1(4) and later 4.0(3) and later 2.3(5)
15600	5.0 and later

- **CSCea16455/CSCea37089/CSCea37185 (SNMP)**

Product	Fixed Releases
15327	4.1(3) and later 4.0(3) and later
15454, 15454 SDH	4.6(0) and later 4.1(3) and later 4.0(3) and later 2.3(5)
15600	Not Affected

- **CSCee27329 (passwd)**

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

The vulnerabilities for the Cisco ONS 15600 platforms are fixed in the Cisco ONS software Release 5.0, which will be available in September 2004.

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 these vulnerabilities for all affected customers.

## Customers with Service Contracts

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

## 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 assistance with the upgrade, which should be free of charge.

## 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)

Please have your product serial number available and give the URL of this notice as evidence of your entitlement to a free software upgrade. Free 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.

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.

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>.

## Workarounds

Apply ACLs (access control lists) on routers / switches / firewalls installed in front of the vulnerable network devices such that TCP/IP traffic destined for the XTC, TCC/TCC+/TCC2, TCCi/TCC2, or TSC control cards on the switches is only allowed from the network management workstations. Refer to <http://www.cisco.com/warp/public/707/tacl.html> for examples on how to apply access control lists (ACLs) on Cisco routers.

Please note, these workarounds will not prevent spoofed IP packets with the source IP address set to that of the network management station from reaching the switch's management interface. For more information on anti-spoofing refer to [http://www.cisco.com/warp/public/707/21.html#sec\\_ip](http://www.cisco.com/warp/public/707/21.html#sec_ip) and <http://www.ietf.org/rfc/rfc2827.txt>. The Unicast Reverse Path Forwarding (Unicast RPF) feature helps to mitigate problems that are caused by malformed or forged IP source addresses that are passing through a router, refer to [http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur\\_c/fothersf/scfrpf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htm).

For the CSCee27329 (passwd) vulnerability ensure that there are no blank passwords set in the user database. Ensure that the CISCO15 userid has a strong password set.

The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code.

## Exploitation and Public Announcements

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

These vulnerabilities were uncovered during Internal stress testing by Cisco except for the malformed ICMP packet vulnerability, which was reported to Cisco by a customer.

## Status of This Notice: FINAL

This Advisory is provided on an "as is" basis and does not imply any kind of guarantee or warranty of any kind. Your use of the information on the Advisory or materials linked from the Advisory is at your own risk. Cisco reserves the right to change or update this notice at anytime.

**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-20040721-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](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)

- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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.

## Revision History

Revision 1.0	2004-July-21	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>.

---

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).