

# Cisco Security Advisory: Cisco ONS15454 and Cisco ONS15327 Vulnerabilities

Advisory ID: cisco-sa-20021031-ons-vulnerability

<http://www.cisco.com/warp/public/707/cisco-sa-20021031-ons-vulnerability.shtml>

## Revision 1.1

Last Updated 2002 November 4 0100 UTC (GMT)

For Public Release 2002 October 31 1600 UTC (GMT)

---

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

---

## Contents

- [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

Multiple vulnerabilities exist in the Cisco ONS15454 optical transport platform and the Cisco ONS15327 edge optical transport platform. All Cisco ONS software releases earlier than 3.4 are vulnerable.

The Cisco ONS15454E is affected only by CSCdx82962.

These vulnerabilities are documented as Cisco bug ID CSCds52295, CSCdt84146, CSCdv62307, CSCdw15690, CSCdx82962 and CSCdy70756. 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-20021031-ons-vulnerability.shtml>.

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

## ☐ **Affected Products**

This section provides details on affected products.

### ☐ **Vulnerable Products**

All Cisco ONS15454 and ONS15327 hardware running Cisco ONS releases earlier than 3.4 are affected by these vulnerabilities.

The Cisco ONS15454E is affected only by CSCdx82962.

To determine your software revision, view the help-about window on the CTC network management software.

### ☐ **Products Confirmed Not Vulnerable**

Hardware not affected includes the 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.

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

## ☐ **Details**

The ONS hardware is managed via the TCC, TCC+, TCCi or the XTC control cards which 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.

These vulnerabilities are documented as Cisco bug ID CSCds52295, CSCdt84146, CSCdv62307, CSCdw15690, CSCdx82962 and CSCdy70756, which requires a CCO account to view and can be viewed after 2002 November 1 at 1600 UTC.

- **CSCds52295** -- It is possible to open a FTP connection to the TCC, TCC+ or XTC using any nonexistent user-name and password. In order to exploit this vulnerability a person must be able to establish a FTP connection to the TCC, TCC+ or XTC.
- **CSCdt84146** -- User-names and passwords are stored in clear text in the running image database of the TCC, TCC+ or XTC. In order to exploit this vulnerability a person needs access to the backup of the image database.

- **CSCdv62307** -- The SNMP community string "public" cannot be changed in the Cisco ONS software. In order to exploit this vulnerability a person must be able to establish a SNMP connection to the TCC, TCC+ or XTC.
- **CSCdw15690** -- Requesting an invalid CORBA Interoperable Object Reference (IOR) via HTTP may cause the TCC, TCC+ or XTC to reset. In order to exploit this vulnerability a person must be able to establish a HTTP connection to the TCC, TCC+ or XTC.
- **CSCdx82962** -- HTTP requests starting with any character other than '/' may cause the TCC, TCC+, TCCi or XTC to reset. In order to exploit this vulnerability a person must be able to establish a HTTP connection to the TCC, TCC+ or XTC
- **CSCdy70756** -- The TCC, TCC+ and XTC have a user-name and password that can be used to gain access to the underlying VxWorks Operating System and it is not possible to change or disable this account. In order to exploit this vulnerability a person must be able to establish a Telnet connection to TCC, TCC+ or XTC.

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

## ☐ Impact

This sections describes the impact of these vulnerabilities.

- **CSCds52295** -- Once a FTP connection has been opened a person could upload modified configuration files and delete software images from the TCC, TCC+ or XTC.
- **CSCdt84146** -- By analyzing an offline database backup of the TCC, TCC+ or XTC, it is possible to extract user-name and password pairs. Using the administrator password a person can access the TCC, TCC+ or XTC either remotely or locally and gain complete control over the Cisco ONS platform.
- **CSCdv62307** -- By using the SNMP read-only community string a person may gain unauthorized access to information in the SNMP MIBs on the TCC, TCC+ or XTC. User-names and passwords cannot be extracted using this method.
- **CSCdw15690** -- By requesting an invalid CORBA IOR object via HTTP a person may cause the TCC, TCC+ or XTC to reset. This does not impact the traffic already flowing through the switch.
- **CSCdx82962** -- By requesting URLs starting with a character other than '/' via HTTP a person may cause the TCC, TCC+, TCCi or XTC to reset. This does not impact the traffic already flowing through the switch.
- **CSCdy70756** -- Using the VxWorks OS account a person can access the TCC, TCC+ or XTC either remotely or locally and gain complete control over the Cisco ONS platform.

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

## ☐ Software Versions and Fixes

All vulnerabilities are fixed in the Cisco ONS software release 3.4 and later for the TCC+ installed in the ONS 15454, the TCCi installed in the ONS 15454E and the XTC installed in the ONS 15327. The Cisco ONS software release 3.2.1 also has all the vulnerabilities fixed in it. For the TCC control cards, the Cisco ONS software release 2.3.3 will be available on CCO on November 4, 2002.

The procedure to upgrade to the fixed software version on the Cisco ONS 15454 is detailed at [http://www.cisco.com/en/US/products/hw/optical/ps2006/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/optical/ps2006/prod_installation_guides_list.html).

The procedure to upgrade to the fixed software version on the Cisco ONS 15327 is detailed at [http://www.cisco.com/en/US/products/hw/optical/ps2001/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/optical/ps2001/prod_installation_guides_list.html).

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

## ☐ Workarounds

This section describes workarounds.

- **CSCds52295** - Restrict FTP traffic to the gateway node(s) with a router configured to restrict FTP access to the TCC, TCC+ or XTC so that FTP access is only allowed from authorized workstations. This can be done by adding Access Control Lists and turning on Unicast Reverse Path Forwarding on the router.  
Please note, this will not prevent spoofed IP packets, from the local segment, with the source IP address set to that of the authorized workstation from reaching the TCC, TCC+ or XTC.
- **CSCdt84146** - It is possible to mitigate the effects of this vulnerability by making sure that the backup Cisco ONS images from the TCC, TCC+ or XTC are secure from unauthorized access.
- **CSCdv62307** - Restrict SNMP traffic to the gateway node(s) with a router configured to restrict SNMP access to the TCC, TCC+ or XTC so that SNMP access is only allowed from valid network management workstations. This can be done by adding Access Control Lists and turning on Unicast Reverse Path Forwarding on the router.  
Please note, this will not prevent spoofed IP packets, from the local segment, with the source IP address set to that of the network management station from reaching the TCC, TCC+ or XTC.
- **CSCdw15690** - Restrict HTTP traffic to the gateway node(s) with a router configured to restrict HTTP access to the TCC, TCC+ or XTC so that HTTP access is only allowed from valid network management workstations. This can be done by adding Access Control Lists and turning on Unicast Reverse Path Forwarding on the router.  
Please note, this will not prevent spoofed IP packets, from the local segment, with the source IP address set to that of the network management station from reaching the TCC, TCC+ or XTC.
- **CSCdx82962** - Restrict HTTP traffic to the gateway node(s) with a router configured to restrict HTTP access to the TCC, TCC+ or XTC so that HTTP access is only allowed from valid network management workstations. This can be done by adding Access Control Lists and turning on Unicast Reverse Path Forwarding on the router.  
Please note, this will not prevent spoofed IP packets, from the local segment, with the source IP address set to that of the network management station from reaching the TCC, TCC+ or XTC.
- **CSCdy70756** - Restrict Telnet traffic to the gateway node(s) with a router configured to restrict Telnet access to the TCC, TCC+ or XTC so that Telnet access is only allowed from authorized workstations. This can be done by adding Access Control Lists and turning on Unicast Reverse Path Forwarding on the router.  
Please note, this will not prevent spoofed IP packets, from the local segment, with the source IP address set to that of the workstation from reaching the TCC, TCC+ or XTC.

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

## ☐ 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.

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

## ☐ **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>.

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

## ☐ **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.

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

## ☐ **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.

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

## ☐ **Exploitation and Public Announcements**

All defects were reported to Cisco by customers. The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

[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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20021031-ons-vulnerability.shtml>.

In addition to worldwide website posting, a text version of this advisory is clear-signed with the Cisco PSIRT PGP key having the fingerprint FEB1 1B89 A64B 60BB 4770 D1CE 93D2 FF06 F236 759C 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-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [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 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	2002- November-04	Documented ONS Release 3.2.1 as also having all the fixes.
Revision 1.0	2002- October-31	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/go/psirt>. This includes instructions for press inquiries regarding Cisco security advisories.

[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)



Send

<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>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)