

Table of Contents

<u>Cisco Security Advisory: Cisco ONS15454, ONS15327, ONS15454SDH, and ONS15600 Nessus Vulnerabilities</u>	1
<u>Revision 2.0</u>	1
<u>Updated 2003 May 28</u>	1
<u>For Public Release 2003 May 01 at 1600 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>	2
<u>Software Versions and Fixes</u>	3
<u>Obtaining Fixed Software</u>	3
<u>Workarounds</u>	4
<u>Exploitation and Public Announcements</u>	4
<u>Status of This Notice: FINAL</u>	4
<u>Distribution</u>	4
<u>Revision History</u>	5
<u>Cisco Security Procedures</u>	5

Cisco Security Advisory: Cisco ONS15454, ONS15327, ONS15454SDH, and ONS15600 Nessus Vulnerabilities

Revision 2.0

Updated 2003 May 28

For Public Release 2003 May 01 at 1600 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

Nessus exposes FTP and Telnet vulnerabilities in the Cisco ONS15454 Optical Transport Platform, the Cisco ONS15327 Edge Optical Transport Platform, the Cisco ONS15454SDH Multiplexer Platform, and the Cisco ONS15600 Multiservice Switching Platform. Cisco ONS15454 hardware running ONS Releases 3.0 through Release 3.4.1, Cisco ONS15327 and ONS15454SDH hardware running ONS Releases 3.3 through Release 3.4.1, and Cisco ONS15600 hardware running ONS Release 1.0 is affected by these vulnerabilities. Nessus is a free security scanner software available from nessus.org.

These vulnerabilities are documented as Cisco Bug IDs CSCdz83515, CSCdz83519, and CSCdz48556. 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-20030501-ons.shtml>.

Affected Products

- Cisco ONS15454 hardware running ONS Releases 3.0 through Release 3.4.1
- Cisco ONS15327 and Cisco ONS15454SDH hardware running ONS Releases 3.3 through Release 3.4.1
- Cisco ONS15600 hardware running ONS Release 1.0

Products *not* affected by these vulnerabilities are listed below.

- Cisco ONS15454 hardware running ONS Releases 4.0 and 2.x
- Cisco ONS15327 hardware running ONS Release 4.0 and Release 1.x
- Cisco ONS15454SDH hardware running ONS Release 4.0

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 network management software.

Details

The affected Cisco ONS15454, ONS15327, ONS15454SDH, and ONS15600 hardware is managed via the TCC+, XTC, TCCi, 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.

DDTS – Description	Details
CSCdz83515 – TCC+ reboots on Nessus VxWorks FTP DoS script	By making an invalid FTP request, a person may cause the TCC+, XTC, TCCi, or TSC control cards to reset. Repeated invalid requests would cause both the control cards to be
CSCdz83519 – TCC+ reboots on Nessus VxWorks binlogin overflow script	reset at the same time. By making an invalid Telnet request, a person may cause the TCC+, XTC, TCCi, or TSC control cards to reset. Repeated invalid requests would cause both the control cards to be
CSCdz48556 – TCC+ reboots due to FTP server input buffer overflow vulnerability	reset at the same time. By making an invalid FTP request, a person may cause the TCC+, XTC, TCCi, or TSC control cards to reset. Repeated invalid requests would cause both the control cards to be

reset at the same time.

These vulnerabilities are documented as Bug IDs CSCdz83515, CSCdz83519, and CSCdz48556. Details can be viewed after 2003 May 02 by accessing the Cisco Bug Toolkit (registered customers only) .

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

Impact

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

On the Cisco ONS15454, ONS15327, and ONS15454SDH hardware platforms, 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 via the TCC+, XTC, and TCCi control cards are not available until the control card reboots.

On the Cisco ONS15600 hardware platforms, 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 via the TSC control cards are not available until the control card reboots.

Software Versions and Fixes

All these vulnerabilities for the ONS15454, ONS15327, and ONS15454SDH platforms are fixed in the Cisco ONS software Releases 4.0 and later for the affected platforms.

All these vulnerabilities for the ONS15600 platforms are fixed in the Cisco ONS software Release 1.1, which will be available in September 2003.

Upgrade procedures can be found as indicated below.

- The procedure to upgrade to the fixed software version on the Cisco ONS15454 hardware is detailed at <http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/r40docs/sftupgrd/index.htm>.
- The procedure to upgrade to the fixed software version on the Cisco ONS15327 hardware is detailed at <http://www.cisco.com/univercd/cc/td/doc/product/ong/15327/327doc40/index.htm>.
- The procedure to upgrade to the fixed software version on the Cisco ONS1600 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 may only install and expect support for the feature sets they have purchased.

Customers with service contracts should contact their regular update channels to obtain the free software upgrade identified via this advisory. For most customers with service contracts, 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> (registered customers only) .

Customers whose Cisco products are provided or maintained through a 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 free software upgrade(s).

Customers who purchased directly 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 obtain fixed software 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).

- +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 advisory as evidence of your entitlement to a free upgrade.

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

Workarounds

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

Use Unicast Reverse Path Forwarding and access control lists on routers and firewalls to allow only valid network management workstations gain FTP and Telnet access to the TCC+, XTC, TCCi, or TSC control cards.

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 reported to PSIRT by internal development testing and customers.

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-20030501-ons.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 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
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- 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 2.0	2003-May-28	Added CSCdz48556. Another vulnerability resolved by the fixed software listed in the advisory.
Revision 1.0	2003-May-01	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>.

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