

Table of Contents

<u>Cisco Security Advisory: Cisco ONS 15216 OADM Telnet Denial-of-Service Vulnerability</u>	1
<u>Document ID: 65541</u>	1
<u>Revision 1.0</u>	1
<u>For Public Release 2005 July 13 1500 UTC (GMT)</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Affected Products</u>	1
<u>Vulnerable Products</u>	1
<u>Products Confirmed Not Vulnerable</u>	2
<u>Details</u>	2
<u>Impact</u>	2
<u>Software Versions and Fixes</u>	2
<u>Obtaining Fixed Software</u>	3
<u>Customers with Service Contracts</u>	3
<u>Customers using Third-party Support Organizations</u>	3
<u>Customers without Service Contracts</u>	3
<u>Workarounds</u>	3
<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 ONS 15216 OADM Telnet Denial-of-Service Vulnerability

Document ID: 65541

Revision 1.0

For Public Release 2005 July 13 1500 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

The Cisco ONS 15216 OADM (Optical Add/Drop Multiplexer) contains a vulnerability in the handling of telnet sessions that can cause a denial-of-service condition in the management plane. Traffic going through the Cisco ONS 15216 OADM (i.e. transit traffic), is not affected when the management plane is under a denial-of-service condition. However, clearing the denial-of-service condition on the management plane requires resetting the device, which impacts transit traffic.

Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability (see the Workarounds section).

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050713-ons.shtml>.

Affected Products

Vulnerable Products

Only the Cisco ONS 15216 OADM running software release 2.2.2 and earlier is affected by the vulnerability described in this advisory.

To determine your software revision, launch a TL1 session and use the **RTRV-NE-GEN** command at the TL1 prompt to retrieve the software version information like in the following example:

```
> RTRV-NE-GEN:<tid>::100;
```

```
TID-000 98-06-20 14-30-00 M001COMPLD"VENDOR=CISCO, MODEL=SOADM-1CH-1530.33,
SN=0001, SOFTWARE=2.0.0, SOFTWAREUPDATE=1-3-2001, FIRMWARE=1.2.7,
FIRMWAREUPDATE=1-3-2001, CHANNUM=1, LAMBDA1=1530.33, ALM-LOSDROP-WEST-1=ON,
ALM-LOSDROP-EAST-1=ON, NAME=SOADM-1, LONGITUDE=100, LATITUDE=45,
IPADDRESS=10.0.0.2, IPMASK=255.0.0.0, A_POWER=OPERATING, B_POWER=OPERATING";
```

This output shows that ONS 15216 OADM is running software release 2.0.0.

Products Confirmed Not Vulnerable

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

Details

Telnet is a protocol used for remote management of network devices. It is defined in RFC 854.

The Cisco ONS15216 OADMs allow service providers to add and drop single to multiple wavelengths from their optical transport network.

The Cisco ONS 15216 OADM has separate management and data planes. The management plane is used to manage the device and is usually connected to a network isolated from the Internet and local to the customer's environment. Traffic being switched and transmitted by the OADM flows through the data plane.

Sending a specially crafted stream of data to a telnet session with the Cisco ONS 15216 OADM can cause the session to lock up, and no further telnet sessions can be established. While the telnet session is locked up, traffic flowing through the data plane is *not affected*. Please note that a TCP session must have been previously established, i.e. the TCP 3-way handshake must have occurred, for the vulnerability to be triggered. This makes it difficult to spoof the source addresses during an attack.

Restoring communications with the management plane requires reloading the Cisco ONS 15216 OADM. This operation affects traffic flowing through the data plane.

This vulnerability is documented in Cisco bug ID CSCee23360 — Communications permanently lost after Telnet session closed.

Impact

Successful exploitation of the vulnerability described in this document may result in a denial-of-service condition in the management plane that will disable the remote manageability of the Cisco ONS 15216 OADM. Clearing a denial-of-service condition on the management plane will result in a denial-of-service condition in the data plane while the device boots up.

Software Versions and Fixes

When considering software upgrades, please also consult http://www.cisco.com/en/US/products/products_security_advisories_listing.html and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") for

Cisco Security Advisory: Cisco ONS 15216 OADM Telnet Denial-of-Service Vulnerability

assistance.

The vulnerability described in this advisory is fixed in **release 2.2.3** and later of the ONS 15216 OADM software. If you are currently running the identified vulnerable software, you should obtain fixed software, as detailed below.

Obtaining Fixed Software

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 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

Please 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.

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

The effectiveness of any workaround 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 is the most appropriate for use in the intended network before it is deployed.

The Cisco ONG platform provides separate management and data planes. Established networking best practices recommend that the management plane is connected to a private network that is completely isolated from the Internet and that is not reachable by customers' traffic.

If complete management and data plane isolation is not possible it is recommended to use Access Control Lists (ACLs) on neighboring routers to only allow telnet connections to the Cisco ONS 15216 OADM from specific network management stations and IP address ranges. This type of filtering could be implemented as part of an Infrastructure ACL, which is a networking best practice. For more information on iACLs, refer to "Protecting Your Core: Infrastructure Protection Access Control Lists" at <http://www.cisco.com/warp/public/707/iacl.html>.

Exploitation and Public Announcements

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

Status of This Notice: FINAL

THIS ADVISORY IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. 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 ANY TIME.

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-20050713-ons.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key 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.grok.org.uk
- 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	2005–July–13	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. 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 © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 13, 2005

Document ID: 65541
