

# Cisco Security Advisory: Cisco Optical Networking System 15000 Series and Cisco Transport Controller Vulnerabilities

Document ID: 69702

Advisory ID: cisco-sa-20060405-ons

<http://www.cisco.com/warp/public/707/cisco-sa-20060405-ons.shtml>

## Revision 1.0

For Public Release 2006 April 05 1500 UTC (GMT)

---

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

---

[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 Optical Networking System (ONS) 15310 Multi-service Provisioning Platforms (MSPP), ONS 15327 MSPP, ONS 15454 MSPP, ONS 15454 Multi-service Transport Platform (MSTP) and the ONS 15600 MSPP. These vulnerabilities will affect Optical nodes that have the Common Control Cards connected to a Data Communications Network (DCN) and are enabled for Internet Protocol Version 4 (IP). Successful exploitation of these vulnerabilities will result in a denial of service (DoS) of the Common Control Cards.

A separate vulnerability exists within the Cisco Transport Controller (CTC) applet launcher which may allow execution of arbitrary code on the CTC workstation. This software is downloaded from the Common Control Cards when a management connection is made to the Optical node.

Cisco has made free software available to address these vulnerabilities for affected customers.

There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060405-ons.shtml>.

# Affected Products

This section provides details on affected products.

## Vulnerable Products

The following Cisco ONS 15000 series platforms are vulnerable, if they are configured for either IP or OSPF on the LAN interface or secure mode EMS-to-network-element access, and if they are running unfixed releases of system software:

- Cisco ONS 15310-CL Series
- Cisco ONS 15327 Series
- Cisco ONS 15454 MSPP
- Cisco ONS 15454 MSTP
- Cisco ONS 15600 Series

Cisco Transport Controller versions 4.0.x and earlier are affected by the CTC vulnerability.

## Products Confirmed Not Vulnerable

The following Cisco ONS 15000 series platforms are not vulnerable to the Cisco ONS vulnerabilities listed above:

- Cisco ONS 15100 Series
- Cisco ONS 15200 Series
- Cisco ONS 15302, ONS 15305 and ONS 15310-MA platforms
- Cisco ONS 15500 Series
- Cisco ONS 15800 Series

Cisco Transport Controller versions 4.1.0 and later are not affected by the CTC vulnerability.

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

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

## Details

The affected Cisco ONS 15310-CL, ONS 15327, ONS 15454 MSPP/ONS 15454 MSTP, and ONS 15600 hardware is managed via the CTX, XTC, TCC2/TCC2+, and TSC control cards respectively (hereafter referred to purely as control card). These control cards are usually connected to a Data Communications Network (DCN). In this context the term DCN is used to denote the network that transports management information between a management station and the network entity (NE). This definition of DCN is sometimes referred to as Management Communication Network (MCN). The DCN is usually physically or logically separated from the customer network and isolated from the Internet. This limits the exposure to the exploitation of these vulnerabilities from the Internet.

## ACK Denial of Service (DoS) Attack

This vulnerability is documented in Cisco bug ID: [CSCei45910](#) ([registered](#) customers only) : ACK Denial of Service (DoS) attack.

This vulnerability applies to all Cisco ONS NEs when IP is configured on the Local Area Network (LAN) interface.

IP on the LAN interface is enabled by default.

NEs which are not enabled for IP on the LAN interface are not affected by this vulnerability.

If an IP address has been entered into the IP address field on the CTC navigation tab, (Provisioning > Network > General), the device is enabled for IP and is vulnerable if running an affected version of software.

The NEs are susceptible to an ACK Denial of Service (DoS) attack on multiple remote management TCP ports. Ports include:

```
80:      HTTP
443:     HTTPS
1080:    SOCKS
2361:    TL1
3081:    TL1-LV
3082:    TL1-RAW
3083:    TL1-TELNET
57790:   non-secure Internet Inter-ORB Protocol (IIOP) port
57791:   Secure Socket Layer Inter-ORB Protocol (SSLIOF) port.
```

**Note:** Not all ports are open in all versions of system software.

The control card(s) on the network entity will exhaust memory resources and be unable to open any new socket connections, and may reset under continued 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. Repeated attacks could cause both control cards to be reset at the same time.

## Control Card Resets with Crafted IP Packet

This vulnerability is documented in Cisco bug ID: [CSCsc51390](#) ([registered](#) customers only) : Control card resets with crafted IP packet.

This vulnerability applies to all Cisco ONS NEs when IP is configured on the LAN interface and secure mode for element management system (EMS)-to-network-element access is enabled. The NEs are susceptible to a DoS attack when receiving a specially crafted IP packet.

NEs which are not enabled for secure mode EMS-to-network-element access are not affected by this vulnerability.

Secure mode EMS-to-network-element access is disabled by default.

A device is vulnerable if via CTC the Provisioning > Security > Access node level navigation tab has Access State checked for `secure`, and is not vulnerable if it is checked for `non-secure`.

Repeated crafted IP packets would cause both the control cards to be reset at the same time.

## Control Card Resets with Crafted IP Packet

This vulnerability is documented in Cisco bug ID: [CSCsd04168](#) ([registered](#) customers only) : Control card resets with crafted IP packet.

This vulnerability applies to all Cisco ONS NEs in which IP is configured on the LAN interface. The NEs are susceptible to a Denial of Service (DoS) attack when receiving a specially crafted IP packet.

NEs which are not enabled for IP on the LAN interface are not affected by this vulnerability.

IP on the LAN interface is enabled by default.

If an IP address has been entered into the IP address field on the CTC navigation tab, (Provisioning > Network > General), the device is enabled for IP and is vulnerable if running an affected version of software.

Repeated crafted IP packets could cause both the control cards to be reset at the same time.

## Malformed OSPF Packets Cause Control Cards to Reset

This vulnerability is documented in Cisco bug ID: [CSCsc54558](#) ([registered](#) customers only) : Malformed OSPF packets cause control cards to reset.

This vulnerability applies to all Cisco ONS NEs if Open Shortest Path First (OSPF) routing protocol is configured on the LAN interface of the control cards.

OSPF is a routing protocol defined by [RFC 2328](#) . It is designed to manage IP routing inside an Autonomous System (AS). OSPF packets use IP protocol number 89.

The vulnerability exists in the processing of OSPF packets that can be exploited to cause a reset of the control cards. Since OSPF needs to process unicast packets as well as multicast packets, this vulnerability can be exploited remotely. It is also possible for an attacker to target multiple systems on the local segment at a time.

NEs which are not enabled with OSPF on the LAN interface are not affected by this vulnerability.

OSPF on the LAN interface is disabled by default.

A device is vulnerable if via CTC the Provisioning > Network > OSPF node level navigation tab has the OSPF Active on LAN check box enabled, and is not vulnerable if the check box is not enabled.

## java.policy Permissions too Broad for CTC Launcher

This vulnerability is documented in bug ID: [CSCea25049](#) ([registered](#) customers only) : java.policy permissions too broad for CTC Launcher.

This vulnerability applies to all workstations that may have had CTC installed on them. CTC is a Java application that is installed in two locations; CTC is stored on the control cards and it is downloaded to the users workstation the first time they log into the NE with a new software release.

During the CTC installation, an entry is made in the Java policy file(s) granting all permission to any software originating from the codeBase, or source at `http://*/fs/LAUNCHER.jar`.

Example:

```
grant codeBase "http://*/fs/LAUNCHER.jar" { permission
java.security.AllPermission; };
```

This may allow arbitrary code to be executed on the CTC computer, should a user of the computer with CTC installed, access any web page which runs Java code from `/fs/LAUNCHER.jar` location.

The Java policy files are the java.policy file(s) in the public Java directories, typically `#{java.home}/lib/security/java.policy` where the Java Plugin is installed, and the `.java.policy` file (note the leading dot) in the user's home directory, typically `#{user.home}/.java.policy`.

In CTC versions 4.1.0 and later the launcher.jar file is signed. Versions 4.1.0 and later will also detect the presence of the java.policy entry and post a dialog box offering the user the option to remove the entry.

## Impact

Successful exploitation of&

- [CSCei45910](#) ([registered](#) customers only) : ACK Denial of Service (DoS) attack
- [CSCsc51390](#) ([registered](#) customers only) : Control card resets with crafted IP Packet
- [CSCsd04168](#) ([registered](#) customers only) : Control card resets with crafted IP Packet
- [CSCsc54558](#) ([registered](#) customers only) : Malformed OSPF packets cause control cards to reset

&will result in the corresponding control cards resetting&

- On the Cisco ONS 15310–CL, ONS 15327 and ONS 15454 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 CTX, XTC, TCC2/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.

Successful exploitation of:

- [CSCea25049](#) ([registered](#) customers only) : java.policy permissions too broad for CTC Launcher. With the insertion of the entry in the Java policy file(s) granting all permission to any software originating from the codeBase, or source at `http://*/fs/LAUNCHER.jar`, the CTC installed workstation is vulnerable to execute malicious code from a remote computer. Once executing the malicious version of LAUNCHER.jar it will allow the program privilege level AllPermission on the CTC installed workstation. This allows the malicious program the ability to delete files, download private information from the CTC installed workstation, modify files on the CTC installed workstation, or load other executables.

## Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> 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") or your contracted maintenance provider for assistance.

Vulnerability	Affected Major Release	First Fixed Release
---------------	------------------------	---------------------

ACK DoS Attack (CSCei45910)	1.X.X	Migrate to 4.1.8.1 or later
	4.0.X or earlier	Migrate to 4.1.8.1 or later
	4.1.X	4.1.8.1
	4.5.X	Migrate to 5.0.6 or later
	4.6.X	4.6.6
	4.7.X	Migrate to 5.0.6 or later
	5.0.X	5.0.6
	6.0.X	Not Vulnerable
	6.2.X	Not Vulnerable
	7.0.X	Not Vulnerable
Crafted IP Packet (CSCsc51390)	4.0.X or earlier	Not Vulnerable
	4.1.X	Not Vulnerable
	4.5.X	Not Vulnerable
	4.6.X	Not Vulnerable
	4.7.X	Not Vulnerable
	5.0.X	Not Vulnerable
	6.0.X	Migrate to 6.2.0 or later
	6.2.X	Not Vulnerable
	7.0.X	Not Vulnerable
Crafted IP Packet (CSCsd04168)	4.1.X or earlier	4.1.8.1
	4.5.x	Not Vulnerable
	4.6.X	Not Vulnerable
	4.7.X	Not Vulnerable
	5.0.X	Not Vulnerable
	6.0.X	Not Vulnerable
	6.2.X	Not Vulnerable
	7.0.X	Not Vulnerable
Malformed OSPF (CSCsc54558)	4.0.X or earlier	Migrate to 4.1.8.1 or later
	4.1.X	4.1.8.1
	4.5.X	Migrate to 6.2.0 or later
	4.6.X	Migrate to 6.2.0 or later

	4.7.0	Migrate to 6.2.0 or later
	5.0.X	Migrate to 6.2.0 or later
	6.0.X	Migrate to 6.2.0 or later
	6.2.X	Not Vulnerable
	7.0.X	Not Vulnerable
CTC (CSCea25049)	1.X.X	Migrate to 4.1.0 or later
	4.0.X or earlier	Migrate to 4.1.0 or later
	4.1.X or later	Not Vulnerable

## Workarounds

This section describes workarounds for these vulnerabilities.

- The following general mitigation actions are relevant for all the listed vulnerabilities:  
Ensuring the DCN is physically or logically separated from the customer network and isolated from the Internet will limit the exposure to the exploitation of these vulnerabilities from the Internet or customer networks.

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

To prevent spoofed IP packets with the source IP address set to that of the network management station from reaching the management interface of the NE, leverage anti-spoofing techniques. For more information on leveraging ACLs for anti-spoofing, refer to <http://www.cisco.com/warp/public/707/21.pdf> and <http://www.ietf.org/rfc/rfc2827.txt>.

The Unicast Reverse Path Forwarding (Unicast RPF) feature helps to mitigate problems that are caused by 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 more information.

- [CSCea25049](#) ([registered](#) customers only) : java.policy permissions too broad for CTC Launcher  
Replace the \* in the policy file entry with the IP address of the CTC login node. Duplicate the entry for multiple login nodes.

Example:

Vulnerable entry within Java.policy files:

```
grant codeBase "http://*/fs/LAUNCHER.jar" { permission
java.security.AllPermission; };
```

Workaround entered within Java.policy files:

```
grant codeBase "http://192.0.2.1/fs/LAUNCHER.jar" { permission
java.security.AllPermission; };
```

- [CSCsc51390](#) ([registered](#) customers only) : Control card resets with crafted IP Packet.  
A possible workaround is to have NEs disabled for secure mode EMS-to-network-element access.



**Caution:** Cisco recommends that any remote management of a NE be conducted over a secure protocol, such as SSH, SSL, or SSLIOP.

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

## 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.

## 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 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.

## 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.

## 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 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.

## Distribution

This advisory is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20060405-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](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org)
- [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.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [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	2006 April 05	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>.

---

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

---

Updated: Apr 05, 2006

Document ID: 69702

---