

[NEWS] Cisco ONS 15327, ONS 15454, ONS 15454 SDH, and ONS 15600 Malformed Packet Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0082.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/22/04

To: list@securiteam.com

Date: 22 Jul 2004 18:01:14 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Cisco ONS 15327, ONS 15454, ONS 15454 SDH, and ONS 15600 Malformed Packet Vulnerabilities

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.

DETAILS

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 that 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/>>
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/>.

Impact:

The malformed packet vulnerabilities could be exploited to launch a DoS attack on the optical device.

The control cards provide the timing for the data channels traversing the switch.

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 the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20040721-ons.shtml#software>
<http://www.cisco.com/warp/public/707/cisco-sa-20040721-ons.shtml#software>.

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> <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> <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.

ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@cisco.com> Cisco Systems Product Security Incident Response Team.

The original article can be found at:

<<http://www.cisco.com/warp/public/707/cisco-sa-20040721-ons.shtml>>

<http://www.cisco.com/warp/public/707/cisco-sa-20040721-ons.shtml>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.