

[NEWS] Cisco CSS 11000 Series Denial of Service (TCP SYN)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0020.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/10/03

To: list@securiteam.com

Date: 10 Aug 2003 16:36:18 +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

Get Thawte's New Step-by-Step SSL Guide for MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get your copy of this new guide now: <http://ad.doubleclick.net/clk;5903126;8265119;j>

Cisco CSS 11000 Series Denial of Service (TCP SYN)

SUMMARY

A heavy storm of TCP SYN packets directed to the circuit address of the CSS can cause DoS on it, high CPU load or even sudden reboots.

The issue is known by Cisco as the ONDM Ping failure (CSCdz00787). On the CS800 chassis the system controller module (SCM) sends ONDM (online diagnostics monitor) pings to each SFP card in order to see if they are alive, if the SCM doesn't get a response in about 30 seconds the SCM will reboot the CS800 and there will be no core.

By attacking the circuit IP address of the CSS with SYN packets the traffic is sent up to the SCM over the internal MADLAN Ethernet interface. If this internal interface becomes overloaded, the ONDM ping request and response traffic can be dropped leading this to an internal DoS since no internal communications are available.

Securiteam: [NEWS] Cisco CSS 11000 Series Denial of Service (TCP SYN)

Any attacker could do this externally with a few sessions of NMap and a cable/ADSL internet connection.

DETAILS

Vulnerable systems:

* Cisco models 11800, 11150 and 11050 with chassis CS800.

Solution:

Upgrade to software release WebNS 5.00.110s or above:

<http://www.cisco.com/en/US/products/hw/contnetw/ps789/prod_release_note09186a008014ee04.html>
http://www.cisco.com/en/US/products/hw/contnetw/ps789/prod_release_note09186a008014ee04.html

ACL's to protect the circuit address are recommended.

ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<<http://www.s21sec.com/en/avisos/s21sec-025-en.txt>>
<http://www.s21sec.com/en/avisos/s21sec-025-en.txt>.

The information has been provided by <<mailto:vul-serv@s21sec.com>> S21SEC.

=====

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.