

Cisco CSS 11000 Series DoS

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-08/0077.html>

From: S21SEC (vul-serv_at_s21seccom.s21sec.com)

Date: 08/07/03

Date: 7 Aug 2003 12:39:13 -0000

To: bugtraq@securityfocus.com

ID: S21SEC-025-en
Title: Cisco CSS 11000 Series DoS
Date: 04/07/2003
Status: Solution available
Scope: Interruption of service, high CPU load.
Platforms: All/Chassis CS800.
Author: ecruz, egarcia, jandre
Location: <http://www.s21sec.com/en/avisos/s21sec-025-en.txt>
Release: External
#####

S 2 1 S E C

<http://www.s21sec.com>

Cisco CSS 11000 Series Denial of service

Description of vulnerability

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

SecurityFocus Bugtraq: Cisco CSS 11000 Series DoS

becomes overloaded
the ONDM ping request and response traffic can be dropped leading this to
an internal DoS
since no internal communications are available.

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

Affected Versions and platforms

This vulnerability affects the 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

AcL's to protect the circuit address are recommended.

Additional information

These vulnerabilities have been found and researched by:

Eduardo Cruz ecruz@s21sec.com
Emilin Garcia egarcia@s21sec.com
Jordi Andre jandre@s21sec.com

You can find the last version of this warning in:

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

And other S21SEC warnings in <http://www.s21sec.com/en/avisos/>