

# Table of Contents

**Cisco Security Notice: Response to BugTraq – Cisco CSS 11000 Series DoS.....1**  
Revision 1.0.....1  
Last Updated 2003 September 7.....1  
Please provide your feedback on this document.....1  
Summary.....1  
Details.....1  
Cisco Security Procedures.....4

# Cisco Security Notice: Response to BugTraq – Cisco CSS 11000 Series DoS

## Revision 1.0

Last Updated 2003 September 7

---

Please provide your feedback on this document.

---

**Summary**  
**Details**  
**Cisco Security Procedures**

---

## Summary

This document is provided to simplify access to Cisco responses to possible product security vulnerability issues posted in public forums for Cisco customers. This does not imply that Cisco perceives each of these issues as an actual product security vulnerability. This notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information on the page or materials linked from this page are at your own risk. Cisco reserves the right to change or update this page without notice at any time.

## Details

Original Report: <http://www.securityfocus.com/archive/1/332284> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/336580> .

```
To: BugTraq
Subject: Re: Cisco CSS 11000 Series DoS
Date: Sep 7 2003 10:13PM
Author: Mike Caudill <mcaudill@cisco.com>
Message-ID: <20030907221308.GA20369@cisco.com>
In-Reply-To: <20030807123913.17492.qmail@wopr.bcn.s21sec.com>
```

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
```

Hello S21Sec,

Apologies for our delay in response, but we have been thoroughly testing and investigating this issue to ensure our response is accurate.

Normally, it is not our policy to comment on customer cases, however, since this has been posted as a Security Advisory that contains inaccurate information, we must respond with the correct details.

It appears that the original customer case was possibly misdiagnosed, leading to the incorrect information in your advisory. Hence the details on the mechanics of this attack are incorrect. We will only correct the defect identifier, upgrade information, affected platform information and workaround details here.

The upgrade listed in the solution section of the advisory will not provide a solution to the problem stated in your advisory. We have been able to reproduce a reload given the instructions in your advisory ONLY on the 11800 platform with a heavy storm of TCP SYN packets sent to the circuit address of the CSS. This problem has been documented in CSCec01994. We are working on delivering a fix for the specific problem (CSCec01994) into the next 5.0 and 6.10 maintenance releases which will be available shortly, possibly by the end of the month.

This problem is seen on the 5.0.2.03 and 6.10 Build 4 versions and is specific to the 11800 platform. It does \*not\* affect the 11150 and 11050 platforms.

Using ACLs on an upstream router to protect the circuit address is recommended as a prevention measure, or workaround. For example, the command

```
access-list 116 deny tcp any <circuit address of CSS>
```

can be used on an upstream router in combination with applying the access-group to an outgoing interface to deny TCP to circuit addresses on the CSS.

Thanks much for posting this information, although working with the Cisco PSIRT in the future on advisories will eliminate this type of confusion and inaccurate information.

We do greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist with Product Security Advisories. Our ultimate goal is to ensure that customers have accurate information on which to base upgrade and workaround decisions and we welcome partnership with researchers towards that goal.

Thanks,

- Mike-

-----BEGIN PGP SIGNATURE-----  
Version: PGP 6.5.2

iQA/AwUBPlujXopjyUnrvVJxEQIQtgCgww98VayXf99hahKND7Cwa4GNVdAAAn09Z  
BzpgOjLY1Lh5dLTuNiLy5BsJ  
=N+45  
-----END PGP SIGNATURE-----

```
> S21SEC <vul-serv s21seccom s21sec com> [2003-08-07 18:30] wrote:  
> #####  
> 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
> 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/
>
> [ ----- End of Included Message ----- ]
```

--

```
-----  
|           ||           ||           | Mike Caudill           | mcaudill cisco com   |  
|           ||           ||           | PSIRT Incident Manager | +1.919.392.2855      |  
|           ||           ||           | DSS PGP: 0xEBBD5271   | +1.919.522.4931 (cell)|  
| ..:|||||:..:|||||:..: | RSA PGP: 0xF482F607   | -----  
| C i s c o S y s t e m s | http://www.cisco.com/go/psirt |  
-----
```

## 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/warp/public/707/sec\\_incident\\_response.shtml](http://www.cisco.com/warp/public/707/sec_incident_response.shtml). 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 © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.