

Table of Contents

<u>Cisco Security Notice: Response to BugTraq – Cisco Secure Content Accelerator Vulnerable to SSL Worm</u>	1
<u>Revision 1.0</u>	1
<u>Last Updated 2002 October 4</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Details</u>	1
<u>Cisco Security Procedures</u>	2

Cisco Security Notice: Response to BugTraq – Cisco Secure Content Accelerator Vulnerable to SSL Worm

Revision 1.0

Last Updated 2002 October 4

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/1/294105> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/294115> .

```
To: BugTraq
Subject: Re: Cisco Secure Content Accelerator vulnerable to SSL worm
Date: Oct 4 2002 8:46PM
Author: Mike Caudill <mcaudill@cisco.com>
Message-ID: <200210042046.g94Kkft26308@rtp-cse-184.cisco.com>
In-Reply-To: <20021003193731.GF24428@alcor.net>
```

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

```
We can confirm the finding made by Matt Zimmerman <mdz@debian.org> for all
older releases of the Cisco Secure Content Accelerator software.
```

```
Cisco has released version 3.2.0.20 of Cisco Secure Content Accelerator
software on September 27, 2002 which resolves the OpenSSL issue.
```

```
The new version of software is available to customers via our website at
```

```
http://www.cisco.com/cgi-bin/tablebuild.pl/cs-conacc
```

```
This problem has been documented in the Release-notes for version 3.2.0.20
online at:
```

http://www.cisco.com/univercd/cc/td/doc/product/webscale/css/css_sca/sca_320/v320b

- -Mike-

```
> Product      : Cisco SCA 11000 Series Secure Content Accelerator
> Product URL  : http://www.cisco.com/warp/customer/cc/pd/cxsr/ps2083/
> CVE         : CAN-2002-0656
> Software release: All current releases
> Vendor status  : PSIRT and TAC notified 2002/09/17, last update 2002/09/24
> Patch status   : No patch available
```

```
> Attempts to exploit the vulnerability described in CAN-2002-0656 cause the
> SCA 11000 (all tested software releases) to spontaneously reboot, resulting
> in at least a denial of service. This product incorporates code from an
> older OpenSSL release, and thus shares the same vulnerability. There is no
> known means to work around this issue, short of disabling SSL services on
> the system.
```

```
> Cisco's Secure Content Accelerator is closely related to SonicWall's SSL
> offloader product. The SonicWall product was also vulnerable, and a
> statement and fix were issued promptly:
```

```
> http://www.sonicwall.com/support/security\_advisories/security\_advisory-openssl.html
```

```
> No official fix is as yet available from Cisco for this issue, and no
> advisory has been released. Impact is likely equivalent to impact on the
> SonicWall product.
```

```
> Cisco PSIRT publishes advisories here:
```

```
> http://www.cisco.com/warp/public/707/advisory.html
```

```
> --
> - mdz
```

--

```
-----
|           ||           ||           | Mike Caudill           | mcaudill cisco com | | | | | | |
|           ||           ||           | PSIRT Incident Manager | 919.392.2855       |
|           ||           ||           | DSS PGP: 0xEBBD5271   | 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 |
-----
```

-----BEGIN PGP SIGNATURE-----

Version: PGP 6.5.2

```
iQA/AwUBPZ3+GYpJyUnrvVJxEQI1bQCeP9Ce2M7rpVgGncXa67XLyUcFzNoAoN5p
8V8uMFPZKxJ10sHmkzOceYc9
=qOdy
```

-----END PGP SIGNATURE-----

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. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at

Cisco Security Notice: Response to BugTraq – Cisco Secure Content Accelerator Vulnerable to SSL Worm

<http://www.cisco.com/go/psirt>.

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.