

Cisco Security Advisory: Cisco OpenSSL Implementation Vulnerability

Revision 1.6

Last Updated 2004 April 8 at 1600 UTC (GMT)

For Public Release 2004 March 17 at 1300 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Obtaining Fixed Software](#)

[Workarounds](#)

[Exploitation and Public Announcements](#)


[Status of This Notice: INTERIM](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

A new vulnerability in the [OpenSSL](#)  implementation for SSL has been announced on March 17, 2004.

An affected network device running an SSL server based on an affected OpenSSL implementation may

be vulnerable to a Denial of Service (DoS) attack. There are workarounds available to mitigate the effects of this vulnerability on Cisco products in the workaround section of this advisory. Cisco is providing fixed software, and recommends that customers upgrade to it when it is available.

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20040317-openssl.shtml>.

Affected Products

The following products have their SSL implementation based on the OpenSSL code and *are affected by this vulnerability.*

- Cisco IOS 12.1(11)E and later in the 12.1E release train for the Cisco 7100 and 7200 Series Routers. *Only crypto images (56i and k2) are vulnerable.*
- Cisco IOS 12.2SY and 12.2ZA release trains for the Cisco Catalyst 6500 Series and Cisco 7600 Series Routers. *Only crypto images (k8, k9 and k91) are vulnerable.*
- Cisco PIX Firewall
- Cisco Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Series and Cisco 7600 Series routers
- Cisco MDS 9000 Series Multilayer Switch
- Cisco Content Service Switch (CSS) 11000 and 11500 series
- Cisco Global Site Selector (GSS) 4480 and 4490
- Cisco Content Service Switch (CSS) Secure Content Accelerator (SCA) versions 1 & 2
- CiscoWorks Common Services (CWCS) version 2.2 and CiscoWorks Common Management Foundation (CMF) version 2.1
- Cisco Access Registrar (CAR)
- Cisco Call Manager (CCM)
- Cisco Okena Stormwatch 3.2
- Cisco Application & Content Networking Software (ACNS)
- Cisco Threat Response (CTR)

The following products have their SSL implementation based on the OpenSSL code and *are not affected by this vulnerability.*

- Cisco Secure Intrusion Detection System (NetRanger) appliance. *This includes the IDS-42xx appliances, NM-CIDS and WS-SVS-IDSM2.*
- Cisco SN 5428 and SN 5428-2 Storage Router
- Cisco CNS Configuration Engine
- Cisco Network Analysis Modules (NAM) for the Cisco Catalyst 6000 and 6500 Series switches and Cisco 7600 Series routers
- Cisco SIP Proxy Server (SPS)
- CiscoWorks 1105 Hosting Solution Engine (HSE)
- CiscoWorks 1105 Wireless LAN Solution Engine (WLSE)

- Cisco Ethernet Subscriber Solution Engine (ESSE)

The following products, which implement SSL, are *not affected* by this vulnerability.

- Cisco VPN 3000 Series Concentrators
- Cisco Secure Socket Layer (SSL) Services Module for the Cisco Catalyst 6500 Series and Cisco 7600 Series routers

CatOS does not implement SSL and is not vulnerable.

No other Cisco products are currently known to be affected by this vulnerability. *This vulnerability is still being actively investigated across Cisco products and status of some products has still not been determined.*

Details

Secure Sockets Layer (SSL), is a protocol used to encrypt the data transferred over a TCP session. SSL in Cisco products is mainly used by the HyperText Transfer Protocol Secure (HTTPS) web service for which the default TCP port is 443. The affected products, listed above, are only vulnerable if they have the HTTPS service enabled and the access to the service is not limited to trusted hosts or network management workstations. They are not vulnerable to transit traffic, only traffic that is destined to them may exploit this vulnerability.

To check if the HTTPS service is enabled one can do the following:

1. Check the configuration on the device to verify the status of the HTTPS service.
2. Try to connect to the device using a standard web browser that supports SSL using a URL similar to **https://ip_address_of_device/**.
3. Try and connect to the default HTTPS port, TCP 443, using Telnet. **telnet ip_address_of_device 443**. If the session connects the service is enabled and accessible.

Testing by the OpenSSL development team has uncovered a null-pointer assignment in the `do_change_cipher_spec()` function. A remote attacker could perform a carefully crafted SSL/TLS handshake against a server that used the OpenSSL library in such a way as to cause OpenSSL to crash. This crash on many Cisco products would cause the device to reload. Repeated exploitation of this vulnerability would result in a Denial of Service (DoS) attack on the device.

Another flaw was also discovered in the SSL/TLS handshaking code when using Kerberos ciphersuites. A remote attacker could perform a carefully crafted SSL/TLS handshake against a server configured to use Kerberos ciphersuites in such a way as to cause OpenSSL to crash. None of the Cisco OpenSSL implementations are known to use Kerberos ciphersuites and are therefore not affected by this second vulnerability.

A third vulnerability described in the NISCC advisory is a bug in older versions of OpenSSL, versions before 0.9.6d, that can also lead to a Denial of Service attack. None of the Cisco OpenSSL implementations are known to be affected by this older OpenSSL issue.

More information on the OpenSSL vulnerability is available at

- **Cisco IOS** - All 12.1(11)E and later IOS software crypto (56i and k2) image releases in the 12.1E release train for the Cisco 7100 and 7200 Series Routers are affected by this vulnerability. All IOS software crypto (k8, k9, and k91) image releases in the 12.2SY and 12.2ZA release trains for the Cisco Catalyst 6500 Series and Cisco 7600 Series Routers are affected by this vulnerability. The SSH implementation in IOS is not dependent on any OpenSSL code. SSH implementations in IOS do not handle certificates, yet, and therefore do not use any SSL code for SSH. OpenSSL in 12.1E, 12.2SY, and 12.2ZA release trains is only used for providing the HTTPS and VPN Device Manager (VDM) services.

This vulnerability is documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug ID CSCee00041.

The HTTPS web service, that uses the OpenSSL code, on the device is disabled by default. The **no ip http secure-server** command may be used to disable the HTTPS web service on the device, if required.

The SSH and IPSec services in IOS are not vulnerable to this vulnerability.

- **Cisco PIX Firewall** - PIX 6.x releases are affected by this vulnerability. PIX 5.x releases do not contain any SSL code and are not vulnerable.

The following three features on the PIX leverage the HTTPS functionality which when enabled makes the PIX vulnerable to this vulnerability.

- PIX Device Manager (PDM) or HTTPS access to the PIX for management
- Cut-through Proxy Authentication of HTTPS sessions and secure Cut-through Proxy Authentication of HTTP sessions. This only affects PIX version 6.3.x.
- Easy VPN Remote User Level Authentication and Secure Unit Authentication. This only affects PIX version 6.3.x.

This vulnerability is documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug ID CSCed90672.

- **Cisco Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Series and Cisco 7600 Series routers** - This vulnerability is documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug ID CSCee02055.
- **Cisco MDS 9000 Series Multilayer Switches** - This vulnerability is documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug ID CSCed96246.
- **Cisco Content Service Switch (CSS) 11000 and 11500 series** - WebNS version 6.x and 7.x are affected by this vulnerability. WebNS version 5.x is not vulnerable to the OpenSSL vulnerabilities. This vulnerability is documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug ID CSCee01234 for SCM and is documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug ID CSCee01240 for the SSL module.
- **Cisco Global Site Selector (GSS) 4480 and 4490** - This vulnerability is documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug ID CSCee01057.
- **Cisco Content Service Switch (CSS) Secure Content Accelerator (SCA) versions 1 & 2** - This vulnerability is documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug ID CSCee07431.

- **CiscoWorks Common Services (CWCS) version 2.2 and CiscoWorks Common Management Foundation (CMF) version 2.1** - This vulnerability is documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug ID CSCsa13748.
- **Cisco Access Registrar (CAR)** - This vulnerability is documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug ID CSCee01956.
- **Cisco Call Manager (CCM)** - Only software versions 4.0.1 and later are affected by this vulnerability. This vulnerability is documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug ID CSCee02193.
- **Cisco Okena Stormwatch 3.2** - This vulnerability is documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug ID CSCee00866.
- **Cisco Application & Content Networking Software (ACNS)** - This vulnerability is documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug ID CSCee03670.
- **Cisco Threat Response (CTR)** - This vulnerability is documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug ID CSCee04888.

The Internetworking Terms and Cisco Systems Acronyms online guides can be found at <http://www.cisco.com/univercd/cc/td/doc/cisintwk/>.

Impact

An affected network device running an SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack.

Software Versions and Fixes

- **Cisco IOS -**

Release Train	Fixed Releases	Availability
12.2ZA	12.2(14)ZA8	No software availability date has been determined yet.
12.2SY	12.2(14)SY4	March 25
12.1E	12.1(13)E14	April 8
	12.1.(19)E7	April 8
	12.1(20)E3	April 26
	12.1(22)E	No software availability date has been determined yet.

- **Cisco PIX Firewall** - The vulnerability is fixed in software releases 6.0(4)102, 6.1(5)102,

6.2(3)107, and 6.3(3)124. These engineering builds may be obtained by contacting the Cisco Technical Assistance Center (TAC). *TAC Contact information is given in the Obtaining Fixed Software section below.*

- **Cisco Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Series and Cisco 7600 Series routers** - The vulnerability is fixed in software release 1.1.3(14) which will be available by Friday, 26 of March, 2004. This engineering builds may be obtained by contacting the Cisco Technical Assistance Center (TAC). *TAC Contact information is given in the Obtaining Fixed Software section below.*
- **Cisco MDS 9000 Series Multilayer Switches** - The vulnerability is fixed in software releases 2.0(0.86) and 1.3(3.33).
- **Cisco Content Service Switch (CSS) 11000 and 11500 series** - The vulnerability is fixed in software releases 6.10.3.04, 7.10.5.07s, 7.20.3.09s, and 7.30.0.08s which will be available by Friday, 2 of April, 2004.
- **Cisco Global Site Selector (GSS) 4480 and 4490** - The vulnerability is fixed in software release 1.1.1.1.0 which will be available by Friday, 2 of April, 2004.
- **Cisco Content Service Switch (CSS) Secure Content Accelerator (SCA) versions 1 & 2** - The vulnerability is fixed in software releases 4.2.0.21 which will be available by Wednesday, 31 of March, 2004.
- **CiscoWorks Common Services (CWCS) version 2.2 and CiscoWorks Common Management Foundation (CMF) version 2.1** - The vulnerability is fixed in the OpenSSL 0.9.7d patch for CiscoWorks Common Services 2.2 which is available on CCO as of Friday, 26 of March, 2004. Users of CiscoWorks Common Management Foundation version 2.1 are urged to upgrade to CiscoWorks Common Services 2.2, please contact Cisco Technical Assistance Center (TAC) for assistance in obtaining this free upgrade. *TAC Contact information is given in the [Obtaining Fixed Software](#) section below.*
- **Cisco Access Registrar (CAR)** - The vulnerability is fixed in software release 3.5.0.12 which will be available by Friday, 26 of March, 2004.
- **Cisco Call Manager (CCM)** - The vulnerability is fixed in software release 4.0(1)ES05 which will be available by Wednesday, 24 of March, 2004. Fixed software release 4.0(1)sr2 will be available in April, 2004. For fixed software release 4.0(2) , no software availability date has been determined yet.
- **Cisco Okena Stormwatch 3.2** - No fixed software release or software availability date has been determined yet.
- **Cisco Application & Content Networking Software (ACNS)** - The vulnerability is fixed in software release 5.0.(11)b8 and 5.1(5) which will be available by Wednesday, 31 of March, 2004.
- **Cisco Threat Response (CTR)** - The vulnerability is fixed in software release 2.0.3 which will be available by Thursday, 1 of April, 2004.

Obtaining Fixed Software

Cisco is offering free software upgrades to address this vulnerability for all affected customers.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, Customers agree to be bound by the terms of Cisco's software license terms found at

<http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at the Cisco Connection Online Software Center at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com/tacpage/sw-center>. To access the software download URL, you must be a [registered](#) user and you must be logged in.

Customers whose Cisco products are provided or maintained through a prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers, should contact that support organization for assistance with obtaining the software upgrade(s).

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC) using the contact information listed below. In these cases, customers are entitled to obtain a free upgrade to a later version of the same release or as indicated by the applicable corrected software version in the Software Versions and Fixes section (noted above).

Cisco TAC contacts are as follows:

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

See <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Please have your product serial number available and give the URL of this notice as evidence of your entitlement to a upgrade. Upgrades for non-contract customers must be requested through the TAC.

Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Workarounds

The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code as soon as it is available.

- Restrict access to the HTTPS server on the network device. Allow access to the network device only from trusted workstations by using access lists / MAC filters that are available on the affected

platforms.

- Disable the SSL server / service on the network device. This workaround must be weighed against the need for secure communications with the vulnerable device.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any malicious use of the vulnerability described in this advisory.

This vulnerability was reported to Cisco PSIRT by NISCC. NISCC has documented this vulnerability at <http://www.uniras.gov.uk/vuls/2004/224012/index.htm> .

Status of This Notice: INTERIM

This is an interim advisory. Although Cisco cannot guarantee the accuracy of all statements in this advisory, all of the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of this advisory unless there is some material change in the facts. Should there be a significant change in the facts, Cisco may update this advisory.

A stand-alone copy or paraphrase of the text of this security advisory that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20040317-openssl.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key having the fingerprint 8C82 5207 0CA9 ED40 1DD2 EE2A 7B31 A8CF 32B6 B590 and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

Revision History

Revision 1.6	2004-April-8	Updated CTR and MDS 9000 fixed release information.
Revision 1.5	2004-April-1	Added details for CWCS. Updated CSS fixed release information.
Revision 1.4	2004-March-26	Added details for CCM and GSS, CSS and SCA.
Revision 1.3	2004-March-23	Change availability date for FWSM. Added details for ACNS.
Revision 1.2	2004-March-19	Added the IOS 12.2ZA release train, CSS SCA, ACNS, CTR, GSS 4490 and the CSS 11500 series to the affected product list. Added more details on the PIX.
Revision 1.1	2004-March-18	Added CCM, Okena Stormwatch as affected. Added SSL module for 6500/7600 as not affected. Elaborated on the IOS releases in the Affected section.
Revision 1.0	2004-March-17	Initial release.

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

This advisory is copyright 2004 by Cisco Systems, Inc. This advisory may be redistributed freely after the release date given at the top of the text, provided that redistributed copies are complete and unmodified, including all date and version information.

[Home](#)[How to Buy](#)[Login](#)[Profile](#)[Feedback](#)[Site Map](#)[Help](#)

All contents are Copyright © 1992-2004 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).