

Cisco Security Advisory: SSL Implementation Vulnerabilities

Document ID: 45643

Advisory ID: cisco-sa-20030930-ssl

<http://www.cisco.com/warp/public/707/cisco-sa-20030930-ssl.shtml>

Revision 2.2

Last Updated 2004 January 21 0030 UTC (GMT)

For Public Release 2003 September 30 2330 UTC (GMT)

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

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of This Notice: INTERIM](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

On September 30, 2003, new vulnerabilities in the [OpenSSL](#) implementation for SSL were announced. This is referred to as the "first" vulnerability in this document.

On November 4, 2003, another vulnerability in the [OpenSSL](#) implementation for SSL, version 0.9.6, was announced. This is referred to as the "second" vulnerability in this document.

An affected network device running an SSL server based on an affected OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack when presented with a malformed certificate by a client. The network device may be vulnerable to this vulnerability even if it is configured to not authenticate certificates from the client. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20030930-ssl.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The following products have their SSL implementation based on the OpenSSL code and may be affected by the first OpenSSL vulnerability.

- Cisco IOS 12.1(11)E and later in the 12.1E release train

Note: Only crypto images (56i and k2) are vulnerable for the Cisco 7100 and 7200 Series Routers.

- Cisco IOS 12.2SX and 12.2SY release trains

Note: Only crypto images (k8, k9 and k91) are vulnerable for the Cisco Catalyst 6500 Series and Cisco 7600 Series Routers.

- Cisco PIX Firewall
- Cisco Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Series and Cisco 7600 Series routers
- Cisco Network Analysis Modules (NAM) for the Cisco Catalyst 6000 and 6500 Series switches and Cisco 7600 Series routers
- Cisco Content Service Switch (CSS) 11000 series
- Cisco Content Service Switch (CSS) Secure Content Accelerator versions 1 & 2
- Cisco Threat Response (CTR)
- Cisco Global Site Selector (GSS) 4480
- Cisco Application & Content Networking Software (ACNS)
- Cisco SN 5428 Storage Router
- CiscoWorks 1105 Hosting Solution Engine (HSE)
- CiscoWorks 1105 Wireless LAN Solution Engine (WLSE)
- CiscoWorks Common Services (CMF)
- Cisco SIP Proxy Server (SPS)
- Cisco Secure Policy Manager (CSPM)

The following products have their SSL implementation based on the OpenSSL code and may be affected by the first and second OpenSSL vulnerabilities.

- Cisco PIX Firewall
- Cisco Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Series and Cisco 7600 Series routers
- Cisco Content Service Switch (CSS) 11000 series – only the SCM is affected
- Cisco SN 5428 Storage Router

Products Confirmed Not Vulnerable

The following products, which implement SSL, are currently known to be *not vulnerable* to the OpenSSL vulnerabilities.

- Cisco VPN 3000 Series Concentrators
- Cisco Secure Intrusion Detection System (NetRanger) appliance. This includes the IDS-42xx appliances, NM-CIDS and WS-SVS-IDSM2.
- Cisco Secure Socket Layer (SSL) Services Module for the Cisco Catalyst 6500 Series and Cisco 7600 Series routers
- Cisco Call Manager

CatOS does not implement SSL and is not vulnerable. No other Cisco products are currently known to be affected by these vulnerabilities.

Details

An affected network device running an SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack when presented with a malformed certificate by a client. The network device is vulnerable to this vulnerability even if it is configured to not authenticate certificates from the client.

More information on the first set of OpenSSL vulnerabilities is available at http://www.openssl.org/news/secadv_20030930.txt . This is referred to as the "first" vulnerability in this document.

More information on the second OpenSSL vulnerability is available at http://www.openssl.org/news/secadv_20031104.txt . This is referred to as the "second" vulnerability in this document.

- 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 the first OpenSSL vulnerability. All IOS software crypto (k8, k9, and k91) image releases in the 12.2SX and 12.2SY release trains for the Cisco Catalyst 6500 Series and Cisco 7600 Series Routers are affected by the first OpenSSL vulnerabilities. The first vulnerability is documented as Bug ID [CSCec46274](#) ([registered customers only](#)) . Cisco IOS is not affected by the second OpenSSL vulnerability. The HTTPS web service, that uses the OpenSSL code, on the device is disabled by default. The command **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 these OpenSSL vulnerabilities.
- Cisco PIX Firewall – PIX 5.x does not contain any SSL code and is not vulnerable. The first vulnerability is documented as Bug ID [CSCec31274](#) ([registered customers only](#)) , and the second vulnerability is documented as Bug ID [CSCec69386](#) ([registered customers only](#)) .
- Cisco Firewall Services Module (FWSM) – The first vulnerability is documented as Bug ID [CSCec45573](#) ([registered customers only](#)) , and the second vulnerability is documented as Bug ID [CSCec79098](#) ([registered customers only](#)) .
- Cisco Network Analysis Modules (NAM) – The first vulnerability is documented as Bug ID [CSCec44573](#) ([registered customers only](#)) . Cisco Network Analysis Modules (NAM) is not affected by the second OpenSSL vulnerability.
- Cisco Content Service Switch (CSS) 11000 series – WebNS version 5.x is not vulnerable to the OpenSSL vulnerabilities. The first vulnerability is documented as Bug ID [CSCec45342](#) ([registered customers only](#)) for WebNS and as Bug ID [CSCec45165](#) ([registered customers only](#)) for the SSL module. The second vulnerability is documented as Bug ID [CSCec82334](#) ([registered customers only](#)) for WebNS. The SSL module is not affected by the second OpenSSL vulnerability.
- Cisco Content Service Switch (CSS) Secure Content Accelerator versions 1 & 2 – The first vulnerability is documented as Bug ID [CSCec48769](#) ([registered customers only](#)) . Cisco Content Service Switch (CSS) Secure Content Accelerator versions 1 & 2 is not affected by the second OpenSSL vulnerability.
- Cisco Threat Response (CTR) – The first vulnerability is documented as Bug IDs [CSCec46555](#) ([registered customers only](#)) and [CSCec45342](#) ([registered customers only](#)) . Cisco Threat Response (CTR) is not affected by the second OpenSSL vulnerability.
- Cisco Global Site Selector (GSS) 4480 – The first vulnerability is documented as Bug ID [CSCec45380](#) ([registered customers only](#)) . Cisco Global Site Selector (GSS) 4480 is not affected by the second OpenSSL vulnerability.
- Cisco Application & Content Networking Software (ACNS) – The first vulnerability is documented as Bug ID [CSCec41413](#) ([registered customers only](#)) . Cisco Application & Content Networking Software (ACNS) is not affected by the second OpenSSL vulnerability.
- Cisco SN 5428 Storage Router – The first vulnerability is documented as Bug ID [CSCec44103](#) ([registered customers only](#)) , and the second vulnerability is documented as Bug ID [CSCec69147](#) ([registered customers only](#)) .

- CiscoWorks 1105 Hosting Solution Engine (HSE) – The first vulnerability is documented as Bug IDs [CSCec38542](#) ([registered](#) customers only) and [CSCec50647](#) ([registered](#) customers only) . CiscoWorks 1105 Hosting Solution Engine (HSE) is not affected by the second OpenSSL vulnerability.
- CiscoWorks 1105 Wireless LAN Solution Engine (WLSE) – The first vulnerability is documented as Bug IDs [CSCec38526](#) ([registered](#) customers only) and [CSCec50640](#) ([registered](#) customers only) . CiscoWorks 1105 Wireless LAN Solution Engine (WLSE) is not affected by the second OpenSSL vulnerability.
- CiscoWorks Common Services (CMF) – Both Solaris and Windows versions of CMF 2.2 and CMF 2.1 are vulnerable. Windows versions of Core 1.0 are also vulnerable. The first vulnerability is documented as Bug ID [CSCec43722](#) ([registered](#) customers only) . CiscoWorks Common Services (CMF) is not affected by the second OpenSSL vulnerability.
- Cisco SIP Proxy Server (SPS) – The first vulnerability is documented as Bug ID [CSCec31901](#) ([registered](#) customers only) . Cisco SIP Proxy Server (SPS) is not affected by the second OpenSSL vulnerability.
- Cisco Secure Policy Manager (CSPM) – The first vulnerability is documented as Bug ID [CSCec61390](#) ([registered](#) customers only) . Cisco Secure Policy Manager (CSPM) is not affected by the second OpenSSL vulnerability.

Impact

An affected network device running an SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack when presented with a malformed certificate by a client regardless of whether it is configured to process client certificates or not.

Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

- Cisco IOS –

Train	Fixed Releases	CCO Availability
12.2S	12.2(14)SY3	November 24, 2003
	12.2(17a)SX1	October 30, 2003
12.1E	12.1(20)E2	January 26, 2004
	12.1(14)E7	October 13, 2003

- Cisco PIX Firewall – The first vulnerability is fixed in software release 6.3(3.102). The second vulnerability is fixed in software release 6.3(3.109). These engineering builds may be obtained by contacting the Cisco Technical Assistance Center (TAC). (Contact information is given in the [Obtaining Fixed Software](#) section.)
- Cisco Firewall Services Module (FWSM) – The first vulnerability is fixed in software release 1.1(3.005). The second vulnerability is fixed in software release 2.1(0.208). These engineering builds may be obtained by contacting the Cisco Technical Assistance Center (TAC). (Contact information is given in the [Obtaining Fixed Software](#) section.)
- Cisco Network Analysis Modules (NAM) – The first vulnerability is fixed in software release 3.1 patch 2. Available via CCO download.
- Cisco Content Service Switch (CSS) 11000 series – The first and second vulnerabilities are fixed in software release 6.10.2.03. CCO availability December 17, 2003. The SSL module in the CSS11000

series device is only vulnerable to the first vulnerability and is fixed in software release 7.20.2.06. CCO availability November 11, 2003.

- Cisco Content Service Switch (CSS) Secure Content Accelerator versions 1 & 2 – The first vulnerability is fixed in software release 4.2.0.19. CCO availability October 15, 2003.
- Cisco Threat Response (CTR) – The first vulnerability is fixed in software release 2.0(2). CCO availability October 13, 2003.
- Cisco Global Site Selector (GSS) 4480 – The first vulnerability is fixed in software release 1.1(0). CCO availability December 7, 2003.
- Cisco Application & Content Networking Software (ACNS) – The first vulnerability is fixed in software release 5.0.7. CCO availability September 30, 2003.
- Cisco SN 5428 Storage Router – The first vulnerability is fixed in software release 3.4(1) and later. CCO availability September 26, 2003. The second vulnerability is fixed in software release 3.4(1.6) and later. CCO availability TBD.
- CiscoWorks 1105 Hosting Solution Engine (HSE) – The first vulnerability is fixed in software release 1.7.3. CCO availability November 21, 2003.
- CiscoWorks 1105 Wireless LAN Solution Engine (WLSE) – The first vulnerability is fixed in software release 2.5. CCO availability October 29, 2003.
- CiscoWorks Common Services (CMF) – CMF patches for the first vulnerability have been created for software release 2.1, 2.2 and 3.0. Available via CCO download.
- Cisco SIP Proxy Server (SPS) – The first vulnerability is fixed in software release 2.2. CCO availability March, 2004.
- Cisco Secure Policy Manager (CSPM) – The first vulnerability is fixed in software release 3.1.10. CCO availability November 21, 2003.

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.

Cisco SIP Proxy Server (SPS) – Disable SSL/TLS functionality. One can do this using the Provisioning GUI. Log in, then select **Farm/Proxies** from the Configuration options. Select **Advanced**, and then the **SIP Server Core** tab. Turn the Enable TLS directive to **Off**.

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

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 Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

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

Customers with Service Contracts

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>.

Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

Customers without Service Contracts

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). 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

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

Refer to <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.

Exploitation and Public Announcements

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

Status of This Notice: INTERIM

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

A stand-alone copy or Paraphrase of the text of this document 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-20030930-ssl.shtml>.

In addition to worldwide website posting, a text version of this advisory 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
- Various internal Cisco mailing lists

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 2.2	2004-21-Jan	Updated fixed release information and availability for multiple products.
Revision 2.1	2003-07-Nov	Clarified products that are known to be affected by the second OpenSSL vulnerability. Added CSS 11000 series (SCM only) as an affected product. Added software availability date for CSPM.
Revision 2.0	2003-04-Nov	Added information on second OpenSSL vulnerability.
Revision 1.3	2003-13-Oct	Added CSPM as affected. Updated SCA and NAM fixed software status.
Revision 1.2	2003-02-Oct	In the "Affected Products" and "Details" sections, added CSA and CTR as being affected. In the "Software Versions and Fixes" section, updated information about affected IOS images.
Revision 1.1	2003-30-Sept	Updated information about affected IOS images.
Revision 1.0	2003-30-Sept	Initial public 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/en/US/products/products_security_vulnerability_policy.html. 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 © 2006–2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

Updated: Jan 21, 2004

Document ID: 45643
