

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)[Security Responses](#)

Cisco Security Response: Multiple Vulnerabilities in OpenSSL library

<http://www.cisco.com/warp/public/707/cisco-sr-20061108-openssl.shtml>

Revision 1.6

Last Updated 2007 July 25 1300 UTC (GMT)

For Public Release 2006 November 08 1600 UTC (GMT)




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

Contents

[Cisco Response](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

This is the Cisco PSIRT response to the multiple security advisories published by The OpenSSL Project. The vulnerabilities are as follows:

- RSA Signature Forgery (CVE-2006-4339), described in http://www.openssl.org/news/secadv_20060905.txt 
- ASN.1 Denial of Service Attacks (CVE-2006-2937, CVE-2006-2940), described in http://www.openssl.org/news/secadv_20060928.txt 
- SSL_get_shared_ciphers() buffer overflow (CVE-2006-3738), also in http://www.openssl.org/news/secadv_20060928.txt 

- SSLv2 Client Crash (CVE-2006-4343), also in http://www.openssl.org/news/secadv_20060928.txt 

As of this publication, there are no workarounds available for any of these vulnerabilities, but it may be possible to mitigate some of the exposure. This Security Response lists the status of each product or application when considered individually. However, in cases where multiple applications are running on the same computer, a vulnerability in one application or component can compromise the entire system. This compromise can then be leveraged against applications that would otherwise be unaffected. Therefore, users must consider all applications when determining their exposure to these vulnerabilities. Cisco strongly recommends that customers update all vulnerable applications and components to provide the greatest protection from the listed vulnerabilities. Cisco will update this document in the event of any changes.

Additional Information

RSA Signature Forgery

During the CRYPTO 2006 conference, which was held August 20-24, 2006, Daniel Bleichenbacher presented a method for forging RSA signatures. The attack requires two conditions to be successful:

- The keys use 3 (three) as one of the RSA exponents.
- The signature verification algorithm has vulnerable implementation.

Notes describing this attack are at <http://www.imc.org/ietf-openpgp/mail-archive/msg14307.html> .

The signature verification implementation vulnerability consists of improper verification of PKCS-1 padded data. Any software with this vulnerability might accept a forged signature, but only if the key that is being forged has 3 (three) as one of the exponents.

ASN.1 Denial of Service Attacks

Two vulnerabilities have been uncovered by an ASN.1 test suite developed by Dr. S. N. Henson. Both of these vulnerabilities, if exploited, can cause denial of service. The vulnerabilities are as follows:

- Parsing of certain invalid ASN.1 structures can result in an infinite loop that can consume system memory. This issue does not affect OpenSSL versions prior to 0.9.7. This is assigned CVE number CVE-2006-2937.
- Specially crafted public keys can take a disproportionate amount of time to be processed. This is assigned CVE number CVE-2006-2940.

SSL_get_shared_ciphers() buffer overflow

A specially crafted list of ciphers can be used to overrun a buffer. This vulnerability has been assigned CVE ID of CVE-2006-3738 and was discovered by Tavis Ormandy and Will Drewry from Google Security Team.

SSLv2 Client Crash

SSL server can send malformed packet during SSLv2 connection negotiation that can crash an SSL client. This vulnerability is assigned CVE ID CVE-2006-4343.

Products Affected by OpenSSL Vulnerabilities

Note: This is not a definitive list. Cisco continues to verify other products and the list will be updated accordingly. The following products are affected by the OpenSSL issues listed in this Security Response:

- **Cisco Global Site Selector (GSS 4480, 4490, 4491, 4492)** — Cisco bug ID is [CSCsg22734](#) ([registered](#) customers only) . The fix is expected in the 2.0(1) release that is targeted for February 2007.
- **Cisco MDS 9500 Multilayer Director** — Cisco bug ID is [CSCsg01963](#) ([registered](#) customers only) . Availability of fixed software has not been determined yet.
- **Cisco IDS** — Cisco bug ID is [CSCsg09619](#) ([registered](#) customers only) . Availability of fixed software has not been determined yet.
- **Cisco ONS 15454** — Cisco bug ID is [CSCsg16571](#) ([registered](#) customers only) . The fix is contained in version 8.0 and later.
- **Cisco Access Registrar** — Cisco bug ID is [CSCsg17943](#) ([registered](#) customers only) . Availability of fixed software has not been determined yet.
- **Cisco Secure ACS** — Cisco bug ID is [CSCsg24311](#) ([registered](#) customers only) . The fix is contained in release 4.1(1) build 23 or later.
- **Cisco Security Agent** — Cisco bug ID is [CSCsg46092](#) ([registered](#) customers only) . Fixed libraries are provided by the following hotfixes 4.5.1.659, 5.0.0.201 and 5.1.0.79.
- **Cisco Call Manager** — Only software releases 4.x and higher are affected. None of the previous releases are vulnerable. Cisco bug IDs are [CSCsg68011](#) ([registered](#) customers only) for 4.x releases, and [CSCsg04397](#) ([registered](#) customers only) and [CSCsg04386](#) ([registered](#) customers only) for 5.1 release. The fixes will be available in upcoming software releases as follows:
 - 4.1(3)sr4c, currently targeted for 2006-Dec-11
 - 4.2(3)sr1, currently targeted for 2006-Dec-11
 - 5.1(1), currently targeted for 2006-Dec-11
- **Cisco Unified Presence Server** — Cisco bug ID [CSCsg51110](#) ([registered](#) customers only) . Fixed software will be available in CUPS 1.0(3), currently targeted for 2006-Nov-16.
- **Cisco Security MARS** — Cisco bug ID is [CSCsg51304](#) ([registered](#) customers only) . The fixes will be available in software release 4.2.3, which is expected in 2006-December.
- **Cisco CSS 11500 Series Content Services Switches** — Cisco bug ID is [CSCek57074](#) ([registered](#) customers only) . Fixed software is available as releases 7.50.3.4S and 8.10.2.6S.
- **Cisco Wireless LAN Controller** — Cisco bug ID is [CSCsg59589](#) ([registered](#) customers only) . The fixes will be available in upcoming software releases as follows:

- 3.2.116.x (release date not determined yet)
- 3.2.171.x (targeted for 2007-January-31)
- 4.0.x (targeted for 2006-Dec-18)
- 4.1 (release date not determined yet)

- **Cisco Application and Content Networking System (ACNS)** — Cisco bug ID is [CSCsf97055](#) ([registered](#) customers only) and [CSCsg55732](#) ([registered](#) customers only) . The fix will be present in 5.5.5 software release. It is expected in 2006-December.

- **Cisco Application Control Engine Module** — Cisco bug ID is [CSCsg36592](#) ([registered](#) customers only) . Fixed software is available in the software release 3.0(0)A1(3b).

- **Cisco Wide Area File Services Software (WAFS)** — Cisco bug IDs are [CSCsg55738](#) ([registered](#) customers only) and [CSCsf97064](#) ([registered](#) customers only) . Availability of fixed software has not been determined yet.

- **Cisco Wide Area Application Services (WAAS) Software** — Cisco bug IDs are [CSCsg55742](#) ([registered](#) customers only) and [CSCsf97077](#) ([registered](#) customers only) . The fix will be present in 4.0.5 software release. It is expected in 2007-February.

- **Cisco SIP Proxy Server** — Cisco bug ID is [CSCsg56292](#) ([registered](#) customers only) . Availability of fixed software has not been determined yet.

- **CiscoWorks Common Services** — Cisco bug IDs are [CSCsg58599](#) ([registered](#) customers only) and [CSCsg58592](#) ([registered](#) customers only) . Some Cisco management products integrate CiscoWorks Common Services into their general installation and runtime environments. To verify, navigate the path **Server Configuration > About the Server > Applications and Versions** in the CiscoWorks Server. Patches for 2.2 and 3.0 are available for download from the CiscoWorks Common Services Patches (Strong Crypto) section.

- **CiscoWorks Common Management Foundation** (CMF was referred to as Common Services before the release of CiscoWorks 3.0) — Cisco bug ID is [CSCsg58607](#) ([registered](#) customers only) . Some Cisco management products integrate CiscoWorks Common Services into their general installation and runtime environments. To verify, navigate the path **Server Configuration > About the Server > Applications and Versions** in the CiscoWorks Server. The fix will be present in 3.1 software release. It is expected in 2006-December.

- **Cisco Guard and Detector** — Cisco bug ID is [CSCsg76448](#) ([registered](#) customers only) . Availability of fixed software has not been determined yet.

Products Not Affected by OpenSSL Vulnerabilities

Note: This list is not a definitive list. Cisco continues to verify other products and the list will be updated accordingly. The following products are confirmed not vulnerable.

- **Cisco IOS**

- **Cisco IOS XR**

- **Cisco IP Interoperability and Collaboration System (IPICS)**

- **Cisco ASA/PIX/FWSM** — While these products contain the OpenSSL libraries, they do not make use of the vulnerable code. Nonetheless, the software library has been updated to avoid any potential issues in the future.
 - For Cisco PIX/ASA, this is tracked by Cisco bug IDs [CSCsg21727](#) ([registered](#) customers only) , [CSCsg52606](#) ([registered](#) customers only) , [CSCsg07425](#) ([registered](#) customers only) , [CSCsh14665](#) ([registered](#) customers only) , and [CSCsg07405](#) ([registered](#) customers only) . Software releases with updated libraries will be 6.3.6, 7.0.7, 7.1.2.26, and 7.2.1.21 and later.
 - For Cisco FWSM, this is tracked by Cisco bug ID [CSCsg52485](#) ([registered](#) customers only) , and the fixed libraries are expected in one of upcoming 3.1 interim releases.
- **Content Services Module with SSL daughtercard (CSM-S) for the Cisco Catalyst 6500 Series**
- **SSL module (SSL-M) for the Cisco Catalyst 6500 Series**
- **Cisco Security Manager**

Workaround

SSL is predominately used for securing HTTP traffic, but is also used to secure other TCP traffic, such as SMTP, POP3, IMAP, and FTP.

Generally speaking, there is no workaround for these issues, but mitigation is possible. By blocking affected protocols at the edge of your network and by allowing only legitimate IP addresses to connect to your devices, it is possible to lower your exposure to these vulnerabilities.

Another option, which could reduce the security of your system, is to revert to non-secure variants of the protocols. In that case, you will not be affected by the vulnerabilities described here, but your traffic will be sent in clear text and, if intercepted, an adversary will be able to read it or even modify it while in transit.

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.

Revision History

Revision 1.6	2007-July-25	Added CSCsh14665 for Cisco PIX/ASA appliances
Revision 1.5	2007-January-16	Products Affected by OpenSSL Vulnerabilities section updated for Cisco Security Agent to remove the sentence, Other supported software releases..., and updated the hotfixes.

Revision 1.4	2006-December-26	Products Affected by OpenSSL Vulnerabilites section updated for Cisco Secure ACS to list fixed software version.
Revision 1.3	2006-December-07	Products Affected by OpenSSL Vulnerabilites section updated for Cisco Call Manager, Cisco Application Control Engine Module, CiscoWorks Common Services, CiscoWorks Common Management Foundation, Cisco Application and Content Networking System (ACNS), and Cisco Wide Area Application Services (WAAS).
Revision 1.2	2006-November-17	Products Affected by OpenSSL Vulnerabilities section updated for Cisco Call Manager, Cisco Guard and Detector, Cisco Wide Area File Services Software (WAFS), and Cisco Wide Area Application Services (WAAS). One product added to the Products Not Affected by OpenSSL Vulnerabilities section.
Revision 1.1	2006-November-14	Products Affected by OpenSSL Vulnerabilities section updated to list Cisco Wireless LAN Controller software release fixes and two products added to the Products Not Affected by OpenSSL Vulnerabilities section.
Revision 1.0	2006-November-08	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>.

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).