

Cisco Security Response: OpenSSL – Potential SSL 2.0 Rollback

Document ID: 68324

<http://www.cisco.com/warp/public/707/cisco-sr-20051202-openssl>

Revision 1.4

Last Updated 2005 December 28 1730 UTC (GMT)

For Public Release 2005 December 02 1600 UTC (GMT)

Please provide your feedback on this document.

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

Cisco Response

This is in response to the OpenSSL Advisory released on 2005–Oct–11. The advisory is posted at http://www.openssl.org/news/secadv_20051011.txt. Some of the Cisco Systems product lines are affected by this vulnerability. The lists are not exhaustive.

Additional Information

Many products use OpenSSL but not all of them are affected. Some products use OpenSSL only for its implementation of various cryptographic functions and are not affected by this vulnerability.

In order to perform a Man-in-The-Middle (MiTM) attack, the attacker must insert themselves in the communication channel between two parties. They will then mimic the intended recipient for both parties. In practical terms, this usually means that the attacker must terminate each session on the host they control and then initiate a new session to the intended recipient.

There are several ways an attacker can perform MiTM attacks, including spoofing DHCP information and sending gratuitous ARPs to the switch. The IP Source Guard and Dynamic ARP Inspection features can be used to block that attack vector.

It may be possible to execute MiTM attacks in wireless networks that use the Extensible Authentication Protocol (EAP). Cisco recommends the use of the Protected EAP (PEAP) protocol to block this particular attack vector.

Another possible vector can be DNS poisoning. This attack vector can be mitigated by using the BIND v9.x DNS software from <http://www.isc.org/> or equivalent.

Affected Products

The following products are affected by this vulnerability:

- **Cisco ASA 5500 and Cisco PIX running 7.x software**
Starting from the release 7.0 Cisco PIX and ASA platforms share the same software. Associated DDTS for both platforms is CSCsc48330.
All Cisco ASA software releases up to 7.0.4.2 are affected. Affected software releases for Cisco PIX are from 7.0.1 to 7.0.4.2 only. The first fixed software for both platforms will be interim release 7.0.4.3. It will be available on 2005–Dec–02.
- **CiscoWorks Common Services (CWCS) version 3.0 and CiscoWorks Common Services (CWCS) version 2.2**
Associated DDTS is CSCsc27533. Point patch for CWCS 2.2 customers should be available by 2005–Dec–07. For CWCS 3.0 customers, the point patch will be available by 2005–Dec–16. This fix will also be integrated in to forthcoming CWCS 3.0.3 release, which is expected to be available for customers during January 2006.
- **Cisco Mainframe Channel Connection (CMCC) – PA–4C–E, PA–1C–E, PA–1C–P, CX–CIP2 tn3270 server**
Associated DDTS is CSCej54402. Software releases up to version 28–22 are affected. The first fixed software release will be 28–23. It is scheduled for release in January 2006.
- **Cisco Global Site Selector (4480, 4490, 4491)**
Associated DDTS is CSCsc33835. Software releases up to version 1.2 are affected. The first fixed release is 1.2(2.2.0). In addition to that, a Sustaining Release 1.1(1.7.0) has been made available and it contains the fix for this issue.
- **Cisco Wireless Control System Software**
Associated DDTS is CSCsc58356. Software release up to version 4.0 are affected. The first fixed software release will be 4.0. It will be available during February 2006.
- **Cisco IOS–XR**
Associated DDTS is CSCek01123. Software releases up to version 3.3 are affected. The first fixed release will be 3.3. It is expected during April 2006. SMU AA01341 is available for IOS–XR 3.2.2 which can be obtained by contacting the TAC.

Products not Affected

The following products are confirmed to be not affected by this vulnerability:

- **Cisco PIX Firewall releases 6.x and below**
Associated DDTS is CSCsc36311. While PIX Firewalls running software version 6.x and below are not affected, this DDTS was opened to make the changes recommended by the OpenSSL team and to prevent the possibility that PIX 6.x becomes vulnerable to this issue in the future.
- **Cisco Catalyst 6500 Series Firewall Services Module**
Associated DDTS is CSCsc34709. While Cisco Catalyst 6500 Series FWSM is not affected this DDTS was opened to prevent possibility that it becomes vulnerable to this issue in the future. The first software release with this fix will be 2.3.
- **Cisco Content Service Switch (CSS) family**
Associated DDTS is CSCej62856. While Cisco CSS is not affected this DDTS was opened to prevent possibility that Cisco CSS becomes vulnerable to this issue in the future.
- **Cisco Call Manager releases 4.x**
Transport Layer Security (TLS), the component that uses OpenSSL, was first introduced in the software release 4.0. Releases prior 4.0 are also not affected.
- **Cisco SIP Proxy Server**
- **Cisco ONS15xxx family**

- Cisco Secure Policy Manager
- Cisco Intrusion Detection System family of products
- Cisco Intrusion Prevention System family of products
- Cisco IOS
- Cisco CatOS
- IP Mobility Client
- Cisco Security Agent
- Cisco MDS 9000 Series Multilayer SAN Switches
- Cisco CTI Object Server (CTI OS)

Other products are being investigated.

Revision History

Revision 1.4	2005–December–28	Updated Affected Products section – "Cisco Global Site Selector" entry.
Revision 1.3	2005–December–19	Updated Affected Products section – "Cisco IOS–XR" entry.
Revision 1.2	2005–December–09	Updated Affected Products section – "Cisco Mainframe Channel Connection (CMCC)" entry.
Revision 1.1	2005–December–07	Updates to Products not Affected section – removed entries for "Common Services (NMTG)" and "Cisco Call Manager."
Revision 1.0	2005–December–02	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: Jun 14, 2007

Document ID: 68324
