Cisco Security Advisory: Transport Layer Security Renegotiation Vulnerability

Advisory ID: cisco-sa-20091109-tls

http://www.cisco.com/warp/public/707/cisco-sa-20091109-tls.shtml

Revision 1.4

Last Updated 2009 December 04 2000 UTC (GMT)

For Public Release 2009 November 9 1600 UTC (GMT)

Please provide your feedback on this document.

Contents

Summary

An industry-wide vulnerability exists in the Transport Layer Security (TLS) protocol that could impact any Cisco product that uses any version of TLS and SSL. The vulnerability exists in how the protocol handles session renegotiation and exposes users to a potential man-in-the-middle attack.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20091109-tls.shtml.

[Expand all sections] [Collapse all sections]

Affected Products

Cisco is currently evaluating products for possible exposure to these TLS issues. Products will only be listed in the Vulnerable Products or Products Confirmed Not Vulnerable sections of this advisory when a final determination about product exposure is made. Products that are not listed in either of these two sections are still being evaluated.

Vulnerable Products

This section will be updated when more information is available. The following products are confirmed to be vulnerable:

- Cisco ACE 4700 Series Application Control Engine Appliances
- Cisco ACE Application Control Engine Module
- Cisco ACE GSS 4400 Series Global Site Selector Appliances
- Cisco ACE Web Application Firewall
- Cisco Wireless Control System
- Cisco Wireless LAN Controller (WLC)
- Cisco Wireless Location Appliance
- CiscoWorks Wireless LAN Solution Engine (WLSE)
- Cisco Digital Media Player
- Cisco Digital Media Manager
- Cisco Access Control Server (ACS)
- CiscoWorks Common Services
- Cisco Telepresence Recording Server
- Cisco IOS Software
- Cisco IOS-XE Software
- Cisco NX-OS Software
- Cisco Video Surveillance Operations Manager Software
- Cisco Video Surveillance Media Server Software
- Cisco ASA 5500 Series Adaptive Security Appliances
- Catalyst 6500 Series and Cisco 7600 Series Firewall Services Module (FWSM)
- Cisco AVS 3120 and 3180 Series Application Velocity System
- Cisco CSS 11500 Series Content Services Switches
  The CSS 11500 Series Content Services Switches are affected by this vulnerability with default configurations. However, the client authentication feature can be enabled as mitigation/solution.
  To enable or disable client authentication on a virtual SSL server, use the **ssl-server <number> authentication** command under the **ssl-proxy-list**.

  Note: By default, client authentication is disabled. After you enable client authentication on the CSS, you must specify a CA certificate that the CSS uses to verify client certificates.

- Cisco Content Switching Module (CSM)
- Cisco Wide Area Application Services (WAAS)

- Cisco Application Networking Manager (ANM)
- Cisco Unified IP Phones
- Cisco ONS 15500 Series
- Cisco Unified Contact Center Products
- Cisco Security Agent (CSA)

Products Confirmed Not Vulnerable

The following products are confirmed not vulnerable:

- Cisco AnyConnect VPN Client
- Cisco Unified MeetingPlace
- Cisco Data Center Network Manager
- Cisco Service Control Subscriber Manager
- Cisco Secure Desktop (CSD)

This section will be updated when more information is available.

Top of the section Close Section

Details

TLS and its predecessor, SSL, are cryptographic protocols that provide security for communications over IP data networks such as the Internet. An industry-wide vulnerability exists in the TLS protocol that could impact any Cisco product that uses any version of TLS and SSL. The vulnerability exists in how the protocol handles session renegotiation and exposes users to a potential man-in-the-middle attack.

The following Cisco Bug IDs are being used to track potential exposure to the SSL and TLS issues. The bugs listed below do not confirm that a product is vulnerable, but rather that the product is under investigation by the appropriate product teams.

Registered Cisco customers can view these bugs via Cisco's Bug Toolkit: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Product	Bug ID
Cisco ACE Web Application Firewall	CSCtd01474
Cisco Adaptive Security Device Manager (ASDM)	CSCtd01491
Cisco AON Software	CSCtd01646
Cisco AON Healthcare for HIPAA and ePrescription	CSCtd01652
Cisco Application and Content Networking System (ACNS) Software	CSCtd01529
Cisco Application Networking Manager	CSCtd01480

Cisco ASA 5500 Series Adaptive Security Appliances	CSCtd00697
Cisco ASA Advanced Inspection and Prevention (AIP) Security Services Module	CSCtd01539
Cisco AVS 3100 Series Application Velocity System	CSCtd26728
Cisco Catalyst 6500 Series SSL Services Module	CSCtd06389
Catalyst 6500 Series and Cisco 7600 Series Firewall Services Module (FWSM)	CSCtd04061
Cisco CSS 11000 Series Content Services Switches	CSCtd01636
Cisco Unified SIP Phones	CSCtd01446
Cisco Data Mobility Manager	CSCtd02642
Cisco Digital Media Manager	CSCtd01692
Cisco Digital Media Players	CSCtd01718
Cisco Emergency Responder	CSCtd02650
Cisco IOS Software	CSCtd00658
Cisco IOS XE Software	CSCtd00658
Cisco IOS XR Software	CSCtd02658
Cisco IP Communicator	CSCtd02662
CATOS	CSCtd00662
Cisco IronPort Appliances	CSCtd02069
Cisco NAC Appliance (Clean Access)	CSCtd01453
Cisco NAC Guest Server	CSCtd01462
Cisco NAC Profiler	CSCtd02716
Cisco Network Analysis Module Software (NAM)	CSCtd02729
Cisco Network Registrar	CSCtd02748
Cisco ONS 15500 Series	CSCtd11877
Cisco Physical Access Gateways	CSCtd02777
Cisco Physical Access Manager	CSCtd03912
Cisco Physical Security ISM	CSCtd03920
Cisco QoS Device Manager	CSCtd03923
Cisco Secure Access Control Server	

(ACS)	CSCtd00725
Cisco Secure Desktop	CSCtd03928
Cisco Secure Services Client	CSCtd03935
Cisco Security Agent CSA	CSCtd02689
Cisco Security Monitoring, Analysis and Response System (MARS)	CSCtd02654
Cisco Unified IP Phones	CSCtd04121
Cisco TelePresence Manager	CSCtd01771
Telepresence for Consumer	CSCtd01752
Cisco TelePresence Recording Server	CSCtd01742
Cisco Network Asset Collector	CSCtd04198
Cisco Unified Communications Manager (CallManager)	CSCtd01282
Cisco Unified Business Attendant Console	CSCtd05731
Cisco Unified Contact Center Enterprise	CSCtd05790
Cisco Unified Contact Center Express	CSCtd05790
Cisco Unified Contact Center Management Portal	CSCtd05755
Cisco Unified Contact Center Products	CSCtd05790
Cisco Unified Department Attendant Console	CSCtd05733
Cisco Unified E-Mail Interaction Manager	CSCtd05756
Cisco Unified Enterprise Attendant Console	CSCtd05735
Cisco Unified Mobility	CSCtd05786
Cisco Unified Mobility Advantage	CSCtd05783
Cisco Unified Operations Manager	CSCtd05784
Cisco Unified Personal Communicator	CSCtd05759
Cisco Unified Presence	CSCtd05791
Cisco Unified Provisioning Manager	CSCtd05777
Cisco Unified Quick Connect	CSCtd05738
Cisco Unified Service Monitor	CSCtd05780

Cisco Unified Service Statistics Manager	CStCd05778
Cisco Unified SIP Proxy	CSCtd05765
Cisco Unity	CSCtd02855
Cisco NX-OS Software	CSCtd00699 and CSCtd00703
Cisco Video Portal	CSCtd04097
Cisco Video Surveillance Media Server Software	CSCtd02831
Cisco Video Surveillance Operations Manager Software	CSCtd02780
Cisco Wide Area Application Services (WAAS)	CSCtd13914
Cisco Wireless Control System	CSCtd01625
Cisco Wireless LAN Controller (WLAN)	CSCtd01611
Cisco Wireless Location Appliance	CSCtd04115
CiscoWorks Common Services Software	CSCtd01597
CiscoWorks Wireless LAN Solution Engine (WLSE)	CSCtd04111

This vulnerability has been assigned the Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-3555.

Top of the section Close Section

Vulnerability Scoring Details

Cisco has provided scores for the vulnerability in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html .

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

http://intellishield.cisco.com/security/alertmanager/cvss .

TLS Renegotiation Vulnerability **Calculate the environmental score of All Cisco Bug IDs**					
CVSS Base Score - **4.3**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	None	Partial	None
CVSS Temporal Score - **4.1**					
Exploitability		Remediation Level		Report Confidence	
Functional		Unavailable		Confirmed	

Top of the section Close Section

Impact

A protocol-level design flaw in the TLS specification allows an attacker to perform a man-in-the-middle (MITM) attack on sessions protected by Transport Layer Security (TLS) and Secure Sockets Layer (SSL). Successful exploitation could allow an attacker to inject data into a legitimate SSL/TLS-protected session and trigger a renegotiation. This may allow the attacker to execute operations on the server using the client's credentials but does not allow the attacker to read, decrypt, or alter encrypted traffic between client and server. While the vulnerability exists within the TLS protocol, the impact of an attack depends on the application protocol running over TLS.

Top of the section Close Section

Software Versions and Fixes

This section will be updated to include fixed software versions for affected Cisco products as they become available.

Top of the section Close Section

Workarounds

Workarounds are being investigated. This section will be updated when more information becomes available.

Top of the section Close Section

Obtaining Fixed Software

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/en/US/docs/general/warranty/English/EU1KEN_.html , or as otherwise set forth at Cisco.com Downloads at http://www.cisco.com/public/sw-center/sw-usingswc.shtml .

Do not contact 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

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

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

Top of the section Close Section

Exploitation and Public Announcements

This vulnerability was initially discovered by Marsh Ray and Steve Dispensa from PhoneFactor, Inc.

Cisco is not aware of any malicious exploitation of this vulnerability.

Proof-of-concept exploit code has been published for this vulnerability.

Top of the section Close Section

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.

Top of the section Close Section

Distribution

This advisory is posted on Cisco's worldwide website at :

http://www.cisco.com/warp/public/707/cisco-sa-20091109-tls.shtml

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- 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.

Top of the section Close Section

Revision History

Revision 1.4	2009-December-4	Details and Impact update
Revision 1.3	2009-December-3	Affected products update
Revision 1.2	2009-November-18	Affected products update
Revision 1.1	2009-November-16	Affected products update
Revision 1.0	2009-November-9	Initial public release

Top of the section Close Section

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.

Top of the section Close Section

Suggestions for improvement:

(256 character limit)

Send