Cisco Security Advisory

OpenSSL Alternative Chains Certificate Forgery Vulnerability (July 2015) Affecting Cisco Products

Medium

Advisory ID: cisco-sa-20150710-openssl
Last Updated: 2015 September 16 16:54 GMT
Published: 2015 July 10 16:00 GMT
Version1.23: Final
Workarounds: See below

CVE-2015-1793

Download CVRF
Download PDF
Email

Summary

On July 9, 2015, the OpenSSL Project released a security advisory detailing a vulnerability affecting applications that verify certificates, including SSL/Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS) clients and SSL/TLS/DTLS servers using client authentication.

Multiple Cisco products incorporate a version of the OpenSSL package affected by this vulnerability that could allow an unauthenticated, remote attacker to cause certain checks on untrusted certificates to be bypassed, enabling the attacker to forge "trusted" certificates that could be used to conduct man-in-the-middle attacks.

This advisory will be updated as additional information becomes available.

Cisco will release free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability may be available.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150710-openssl

Affected Products

The bugs are accessible through the Cisco Bug Search Tool and will contain additional platform-specific information, including workarounds (if available) and fixed software versions.

Vulnerable Products

The following Cisco products have been confirmed to be impacted by one or more of the vulnerabilities contained in the July 10, 2015, OpenSSL Project security advisory:

Product	Defect	Fixed releases availability
Collaboration and Social Media		
Cisco SocialMiner	CSCuv26844	11.5.1 (1-May-2016)
Cisco WebEx Node for MCS	CSCuv26109	
Endpoint Clients and Client Software		
Cisco Agent for OpenFlow	CSCuv26243	Patch file available for affected releases.
Cisco Jabber Software Development Kit	CSCuv26303	11.0(0) (26-Aug-2015)
Network and Content Security Devices		
Cisco ASA CX and Cisco Prime Security Manager	CSCuv26213	9.3.3.4 (MR6) (Sep 2015)
Cisco Virtual Security Gateway for Microsoft Hyper-V	CSCuv26137	5.2(1)VSG2(1.4) (31-Oct-2015)
Network Management and Provisioning		
Cisco Packet Tracer	CSCuv26183	7.0 (18-Dec-2015)
Cisco Prime Access Registrar	CSCuv26150	7.0.1 (Oct 2015) 6.1.3 (Oct 2015)
Cisco Prime Collaboration Deployment	CSCuv26283	11.5.1 (Mar 2016)
Cisco Prime Collaboration Provisioning	CSCuv26164	10.6 (31-Jul-2015) 10.5.1 (31-Jul-2015) 10.0 (31-Jul-2015) 9.5 (31-Jul-2015)
Cisco Prime License Manager	CSCuv26185	11.0.1 (Oct 2015) 10.5.2 (Dec 2015)
Cisco Prime Network Services Controller	CSCuv26168	3.4.1c (20-Aug-2015)
Cisco Prime Security Manager	CSCuv26209	9.3.4.2-4 (29-Aug-2015)
Cisco Security Manager	CSCuv26167	4.8 SP1 (31-Jul-2015) 4.9 (31-Aug-2015)
Local Collector Appliance (LCA)	CSCuv26267	2.2.10 (7-Aug-2015)
Routing and Switching - Enterprise and Service Provider		
Cisco 910 Industrial Router	CSCuv26253	1.2.1RB3 (20-Aug-2015)
Cisco IOS-XE (WebUI feature only)	CSCuu82763	XE3.13 14 15 16 (Available) XE3.11 13 (Next Release)
Cisco Nexus 9000 (ACI/Fabric Switch)	CSCuv26128	11.1.2 (Aug 2015)
Unified Computing		
Cisco Virtual Security Gateway	CSCuv26136	5.2(1)VSG2(1.3a) (30-Dec-2015)
Voice and Unified Communications Devices		
Cisco Emergency Responder	CSCuv26293	11.5 (Feb 2016)
Cisco IM and Presence Service (CUPS)	CSCuv26296	
Cisco MediaSense	CSCuv26316	11.5 (20-Oct-2015) 11.0 (20-Oct-2015) 10.5 (20-Oct-2015)
Cisco Unified Attendant Console Standard	CSCuv26279	11.0(2) (30-Sept-2015)
Video, Streaming, TelePresence, and Transcoding Devices		
Cisco Digital Media Players (DMP) 4300 Series	CSCuv26173	5.4(1)RB(2P4) 5.3(6)RB(2P3)
Cisco Digital Media Players (DMP) 4400 Series	CSCuv26173	5.4(1)RB(2P4) 5.3(6)RB(2P3)
Cisco Digital Media Players	CSCuv46148	5.4(1)RB(2P4) 5.3(6)RB(2P3)
Cisco Model D9485 DAVIC QPSK	CSCuv26259	1.2.19 (31-Jul-2015)
Cisco TelePresence Conductor	CSCuv26172	XC4.0 (29-Jul-2015)
Cisco Videoscape Control Suite	CSCuv33644	Patch file available for affected releases (20-Jul-2015)
Cisco Hosted Services		
Cisco Registered Envelope Service (CRES)	CSCuv26099	4.4.1 (1-Aug-2015)
Cisco Universal Small Cell 5000 Series running V3.4.2.x software	CSCuv26256	BV3.4.4.8
Cisco Universal Small Cell 7000 Series running V3.4.2.x software	CSCuv26256	BV3.4.4.8
Cisco WebEx Messenger Service	CSCuv26116	7.9.9 EP1 (Available)
Network Performance Analytics (NPA)	CSCuv26268	1.11.3 (30-Sept-2015)
Partner Supporting Service (PSS) 1.x	CSCuv26208	
Services Analytic Platform	CSCuv26091	Patch file available for affected release.

Products Confirmed Not Vulnerable

Cisco has confirmed that the following products are not vulnerable to the vulnerability announced by the OpenSSL Project on July 9, 2015:

Collaboration and Social Media

- Cisco WebEx Meetings Server versions 1.x
- Cisco WebEx Meetings Server versions 2.x

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Related Resources

IS OpenSSL Alternative Chains Certificate Forgery Bypass Vulnerability

ST 35111

ST 35307

Subscribe to Cisco Security Notifications

Subscribe

Endpoint Clients and Client Software

- Cisco AnyConnect Secure Mobility Client for Android
- Cisco AnyConnect Secure Mobility Client for Linux
- Cisco AnyConnect Secure Mobility Client for Windows
- Cisco AnyConnect Secure Mobility Client for iOS
- Cisco IP Communicator
- Cisco Jabber Guest 10.0(2)
- Cisco Jabber for Android
- Cisco Jabber for Mac
- Cisco Jabber for Windows
- Cisco Jabber for iOS
- Cisco NAC Agent for Mac
- Cisco NAC Agent for Web
- Cisco NAC Agent for Windows
- Cisco UC Integration for Microsoft Lync
- Cisco Unified Personal Communicator
- Cisco WebEx Meetings Client - Hosted
- Cisco WebEx Meetings Client - On Premises
- Cisco WebEx Meetings for Android
- Cisco WebEx Meetings for Blackberry
- Cisco WebEx Productivity Tools
- WebEx Meetings Server - SSL Gateway
- WebEx Recording Playback Client

Network Application, Service, and Acceleration

- Cisco ACE 30 Application Control Engine Module
- Cisco ACE 4710 Application Control Engine (A5)
- Cisco ACE GSS 4400 Series Global Site Selector
- Cisco Application and Content Networking System (ACNS)
- Cisco Extensible Network Controller (XNC)
- Cisco InTracer
- Cisco Network Admission Control (NAC)
- Cisco Nexus Data Broker (NDB)
- Cisco Visual Quality Experience Server
- Cisco Visual Quality Experience Tools Server
- Cisco Wide Area Application Services (WAAS)

Network and Content Security Devices

- Cisco ASA Content Security and Control (CSC) Security Services Module
- Cisco Adaptive Security Appliance (ASA)
- Cisco Adaptive Security Device Manager
- Cisco Clean Access Manager
- Cisco Content Security Appliance Updater Servers
- Cisco Content Security Management Appliance (SMA)
- Cisco Email Security Appliance (ESA)
- Cisco FireSIGHT System Software
- Cisco IPS
- Cisco Identity Services Engine (ISE)
- Cisco IronPort Encryption Appliance (IEA)
- Cisco NAC Guest Server
- Cisco NAC Server
- Cisco Physical Access Control Gateway
- Cisco Physical Access Manager
- Cisco Secure Access Control Server (ACS)
- Cisco Web Security Appliance (WSA)

Network Management and Provisioning

- Cisco Application Networking Manager
- Cisco Cloupia Unified Infrastructure Controller
- Cisco Configuration Professional
- Cisco Connected Grid Device Manager
- Cisco Connected Grid Network Management System
- Cisco Digital Media Manager
- Cisco Insight Reporter
- Cisco Linear Stream Manager
- Cisco MGC Node Manager (CMNM)
- Cisco Multicast Manager
- Cisco Netflow Collection Agent
- Cisco Network Analysis Module
- Cisco Prime Analytics
- Cisco Prime Cable Provisioning
- Cisco Prime Central for SPs
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Manager
- Cisco Prime Data Center Network Manager (DCNM)
- Cisco Prime Home
- Cisco Prime IP Express
- Cisco Prime Infrastructure Standalone Plug and Play Gateway
- Cisco Prime Infrastructure
- Cisco Prime LAN Management Solution (LMS - Solaris)
- Cisco Prime Network Registrar (CPNR)
- Cisco Prime Network
- Cisco Prime Optical for SPs
- Cisco Prime Performance Manager
- Cisco Prime Provisioning for SPs
- Cisco Prime Provisioning
- Cisco Show and Share (SnS)
- Cisco UCS Central
- Cisco Unified Intelligence Center
- Cisco Unified Provisioning Manager (CUPM)
- CiscoWorks Network Compliance Manager

Routing and Switching - Enterprise and Service Provider

- Cisco ASR 5000 Series
- Cisco Application Policy Infrastructure Controller (APIC)
- Cisco Broadband Access Center Telco Wireless
- Cisco Connected Grid Router - CGOS
- Cisco IOS Software and Cisco IOS-XE Software
- Cisco IOS-XE (SSLVPN feature)
- Cisco IOS-XR
- Cisco MDS 9000 Series Multilayer Switches
- Cisco Mobile Wireless Transport Manager
- Cisco Nexus 1000V InterCloud
- Cisco Nexus 1000V Series Switches
- Cisco Nexus 2000 Series FEX
- Cisco Nexus 3X00 Series Switches
- Cisco Nexus 4000 Series Blade Switches
- Cisco Nexus 5000 Series Switches
- Cisco Nexus 6000 Series Switches
- Cisco Nexus 7000 Series Switches
- Cisco Nexus 9000 Series (standalone, running NxOS)
- Cisco ONS 15454 Series Multiservice Provisioning Platforms
- Cisco OnePK All-in-One VM
- Cisco Service Control Operating System

Routing and Switching - Small Business

- Cisco Sx220 switches
- Cisco Sx300 switches
- Cisco Sx500 switches

Unified Computing

- Cisco Common Services Platform Collector
- Cisco Standalone rack server CIMC
- Cisco UCS Invicta Series Solid State Systems
- Cisco Unified Computing System (Management software)
- Cisco Unified Computing System B-Series (Blade) Servers
- Cisco Virtualization Experience Media Engine

Voice and Unified Communications Devices

- Cisco 190 ATA Series Analog Terminal Adaptor
- Cisco 8800 Series IP Phones - VPN Feature
- Cisco ATA 187 Analog Telephone Adaptor
- Cisco Agent Desktop for Cisco Unified Contact Center Express
- Cisco Agent Desktop
- Cisco Billing and Measurements Server
- Cisco Computer Telephony Integration Object Server (CTIOS)
- Cisco DX Series IP Phones
- Cisco Finesse
- Cisco Hosted Collaboration Mediation Fulfillment
- Cisco IP Interoperability and Collaboration System (IPICS)
- Cisco MeetingPlace
- Cisco Packaged Contact Center Enterprise
- Cisco Paging Server (Informacast)
- Cisco Paging Server
- Cisco Remote Silent Monitoring
- Cisco SPA112 2-Port Phone Adapter
- Cisco SPA122 ATA with Router
- Cisco SPA232D Multi-Line DECT ATA
- Cisco SPA30X Series IP Phones
- Cisco SPA50X Series IP Phones
- Cisco SPA51X Series IP Phones
- Cisco SPA525G
- Cisco SPA8000 8-port IP Telephony Gateway
- Cisco SPA8800 IP Telephony Gateway with 4 FXS and 4 FXO Ports
- Cisco TAPI Service Provider (TSP)
- Cisco USC8088
- Cisco Unified 3900 series IP Phones
- Cisco Unified 6901 IP Phones
- Cisco Unified 6911 IP Phones
- Cisco Unified 6921 IP Phones
- Cisco Unified 6945 IP Phones
- Cisco Unified 7800 Series IP Phones
- Cisco Unified 8831 series IP Conference Phone
- Cisco Unified 8945 IP Phone
- Cisco Unified 8961 IP Phone
- Cisco Unified 9951 IP Phone
- Cisco Unified 9971 IP Phone
- Cisco Unified Attendant Console Advanced
- Cisco Unified Attendant Console Business Edition
- Cisco Unified Attendant Console Department Edition
- Cisco Unified Attendant Console Enterprise Edition
- Cisco Unified Attendant Console Premium Edition
- Cisco Unified Client Services Framework
- Cisco Unified Communications Domain Manager
- Cisco Unified Communications Manager (UCM)
- Cisco Unified Communications Manager Session Management Edition (SME)
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- Cisco Unified E-Mail Interaction Manager
- Cisco Unified IP Conference Phone 8831 for Third-Party Call Control
- Cisco Unified IP Phone 7900 Series
- Cisco Unified Integration for IBM Sametime
- Cisco Unified Intelligent Contact Management Enterprise
- Cisco Unified Operations Manager (CUOM)
- Cisco Unified Sip Proxy
- Cisco Unified Web Interaction Manager
- Cisco Unified Workforce Optimization
- Cisco Unity Connection (UC)
- Cisco Unity Connection
- Cisco Virtual PGW 2200 Softswitch
- Cisco Voice Portal (CVP)
- xony VIM/CCDM/CCMP

Video, Streaming, TelePresence, and Transcoding Devices

- Cisco AnyRes Live (CAL)
- Cisco AnyRes VOD (CAL)
- Cisco D9824 Advanced Multi Decryption Receiver
- Cisco D9854/D9854-I Advanced Program Receiver
- Cisco D9858 Advanced Receiver Transcoder
- Cisco D9859 Advanced Receiver Transcoder
- Cisco D9865 Satellite Receiver
- Cisco DCM Series 9900-Digital Content Manager
- Cisco Edge 300 Digital Media Player
- Cisco Edge 340 Digital Media Player
- Cisco Enterprise Content Delivery System (ECDS)
- Cisco Expressway Series
- Cisco Headend System Release
- Cisco Internet Streamer (CDS)
- Cisco Jabber Video for TelePresence (Movi)
- Cisco Media Experience Engines (MXE)
- Cisco Media Services Interface
- Cisco TelePresence 1310
- Cisco TelePresence Advanced Media Gateway Series
- Cisco TelePresence Content Server (TCS)
- Cisco TelePresence EX Series
- Cisco TelePresence Exchange System (CTX)
- Cisco TelePresence ISDN GW 3241
- Cisco TelePresence ISDN GW MSE 8321
- Cisco TelePresence ISDN Link
- Cisco TelePresence MCU (8510, 8420, 4200, 4500 and 5300)
- Cisco TelePresence MX Series
- Cisco TelePresence Management Suite (TMS)
- Cisco TelePresence Management Suite Analytics Extension (TMSAE)
- Cisco TelePresence Management Suite Extension (TMSXE)
- Cisco TelePresence Management Suite Extension for IBM
- Cisco TelePresence Management Suite Provisioning Extension
- Cisco TelePresence Profile Series
- Cisco TelePresence SX Series
- Cisco TelePresence Serial Gateway Series
- Cisco TelePresence Server 8710, 7010
- Cisco TelePresence Server on Multiparty Media 310, 320
- Cisco TelePresence Server on Virtual Machine
- Cisco TelePresence Supervisor MSE 8050
- Cisco TelePresence System 1000
- Cisco TelePresence System 1100
- Cisco TelePresence System 1300
- Cisco TelePresence System 3000 Series
- Cisco TelePresence System 500-32
- Cisco TelePresence System 500-37
- Cisco TelePresence TX 9000 Series
- Cisco TelePresence Video Communication Server (VCS)
- Cisco Telepresence Integrator C Series
- Cisco VDS Service Broker
- Cisco VEN501 Wireless Access Point
- Cisco Video Surveillance 3000 Series IP Cameras
- Cisco Video Surveillance 4000 Series High-Definition IP Cameras
- Cisco Video Surveillance 4300E/4500E High-Definition IP Cameras
- Cisco Video Surveillance 6000 Series IP Cameras
- Cisco Video Surveillance 7000 Series IP Cameras
- Cisco Video Surveillance Media Server
- Cisco Video Surveillance PTZ IP Cameras
- Cloud Object Store (COS)
- Tandberg Codian ISDN GW 3210/3220/3240
- Tandberg Codian MSE 8320 model

Wireless

- Cisco Mobility Services Engine (MSE)
- Cisco Wireless Control System (WCS)
- Cisco Wireless LAN Controller (WLC)

Cisco Hosted Services

- Cisco Cloud Web Security
- Cisco Intelligent Automation for Cloud
- Cisco Proactive Network Operations Center

- Cisco SmartConnection
- Cisco SmartReports
- Cisco Unified Services Delivery Platform (CUSDP)
- Cisco WebEx Meetings (Meeting Center, Training Center, Event Center, Support Center)
- Communication/Collaboration Sizing Tool, Virtue Machine Placement Tool, Cisco Unified Communications Upgrade Readiness Assessment
- Connected Analytics for Network Deployment (CAND)
- Life Cycle Management Agent Manager (LCM)
- Serial Number Assessment Service (SNAS)

No other Cisco products are currently known to be affected by this vulnerability.

Details

The OpenSSL Project disclosed a vulnerability on July 9, 2015. This vulnerability affects both client and server installations of OpenSSL.

OpenSSL Alternative Chains Certificate Forgery Vulnerability

OpenSSL contains a vulnerability that could allow an unauthenticated, remote attacker to cause certain checks on untrusted certificates to be bypassed, enabling the attacker to forge "trusted" certificates that could be used to conduct man-in-the-middle attacks.

The vulnerability is due to an error in the implementation of the logic for finding an alternative certificate chain if the first attempt to build such a chain fails. An unauthenticated, remote attacker could exploit the vulnerability by submitting a crafted certificate chain to an affected device during SSL, TLS, or DTLS authentication. A successful exploit could allow the attacker to cause certain checks on untrusted certificates to be bypassed, enabling the attacker to forge "trusted" certificates that could be used to conduct man-in-the-middle attacks.

The impact of this vulnerability on Cisco products may vary depending on the affected product.

For Cisco products, please refer to the information provided in the Cisco bug IDs listed in the Affected Products section of this document. Additional information and detailed instructions are available in the Cisco installation, configuration, and maintenance guides for each product. If additional clarification or advice is needed, please contact your support organization.

This vulnerability has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2015-1793.

Workarounds

For potential workarounds on a specific Cisco product, refer to the Cisco bug ID, which is available from the Cisco Bug Search Tool.

Fixed Software

When considering software upgrades, customers are advised to consult the Cisco Security Advisories, Responses, and Alerts archive at http://www.cisco.com/go/psirt and review subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

This vulnerability was publicly disclosed by the OpenSSL Project on July 9, 2015.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150710-openssl

---

Revision History

Revision 1.23	2015-September-16	Updated Affected Products section - Vulnerable/Not Vulnerable Products. The following three products moved from Vulnerable to Not Vulnerable: Cisco Nexus 6000 Series Switches, Cisco Nexus 5000 Series Switches, Cisco Nexus 2000 Series FEX.
Revision 1.22	2015-September-14	Updated Affected Products section - Vulnerable/Not Vulnerable Products. The following three products moved from Vulnerable to Not Vulnerable: Cisco Jabber for Android, WebEx Recording Playback Client, and Cisco WebEx Meetings Client - Hosted.
Revision 1.21	2015-August-29	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.20	2015-August-25	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.19	2015-August-21	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.18	2015-August-18	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.17	2015-August-13	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.16	2015-August-07	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.15	2015-August-04	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.14	2015-July-31	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.13	2015-July-29	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.12	2015-July-28	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.11	2015-July-27	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.10	2015-July-24	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.9	2015-July-23	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.8	2015-July-22	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.7	2015-July-21	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.6	2015-July-20	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.5	2015-July-17	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.4	2015-July-16	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.3	2015-July-15	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.2	2015-July-14	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.1	2015-July-13	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
Revision 1.0	2015-July-10	Initial public release.

Legal Disclaimer

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.

A stand-alone copy or paraphrase of the text of this document that omits the distribution URL is an uncontrolled copy, and may lack important information or contain factual errors. The information in this document is intended for end-users of Cisco products.