Cisco Security Advisory

Multiple Vulnerabilities in OpenSSL (June 2015) Affecting Cisco Products

High

Advisory ID: cisco-sa-20150612-openssl
Last Updated: 2017 January 17 14:55 GMT
Published: 2015 June 12 16:00 GMT
Version1.17: Final
CVSS Score: Base - 7.8
Workarounds: Yes

CVE-2014-8176
CVE-2015-1788
CVE-2015-1789
CVE-2015-1790
CVE-2015-1791
CVE-2015-1792
CWE-119
CWE-20
CWE-399

Download CVRF
Download PDF
Email

Summary

On June 11, 2015, the OpenSSL Project released a security advisory detailing six distinct vulnerabilities, and another fix that provides hardening protections against exploits as described in the Logjam research.

Multiple Cisco products incorporate a version of the OpenSSL package affected by one or more vulnerabilities that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or corrupt portions of OpenSSL process memory.

This advisory will be updated as additional information becomes available.

Cisco will release software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities may be available.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150612-openssl

Affected Products

The bugs will be 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 six distinct vulnerabilities contained in the June 11, 2015, OpenSSL Project security advisory:

11.1(2)

Product	Defect	Fixed releases availability
Collaboration and Social Media		
Cisco WebEx Meetings Server versions 1.x	CSCuu82698	2.0.1.915 and later
Cisco WebEx Meetings Server versions 2.x	CSCuu82698	2.0.1.915 and later
Cisco WebEx Node for MCS	CSCuu82686	3.12.9.1 (July 2015)
Cisco WebEx Social	CSCuu82594	No additional releases are planned.
Endpoint Clients and Client Software		
Cisco Agent for OpenFlow	CSCuu82738	4.002 (TBD)
Cisco AnyConnect Secure Mobility Client for Android	CSCuu83398	A patch will be available July 2015.
Cisco AnyConnect Secure Mobility Client for Linux	CSCuu83398	A patch will be available July 2015.
Cisco AnyConnect Secure Mobility Client for Windows	CSCuu83398	A patch will be available July 2015.
Cisco AnyConnect Secure Mobility Client for iOS	CSCuu83398	A patch will be available July 2015.
Cisco Jabber Guest 10.0(2)	CSCuu83421	10.7 (TBD)
Cisco Jabber Software Development Kit	CSCuu82560	11.0(0) (26-Aug-2015)
Cisco Jabber for Android	CSCuu83433	11.0 (TBD)
Cisco Jabber for Mac	CSCuu82558	11.0(1) (TBD)
Cisco Jabber for Windows	CSCuu82561	11.0 (July 2015)
Cisco Jabber for iOS	CSCuu82555	11.0 (Aug. 2015)
Cisco WebEx Meetings Client - Hosted	CSCuu83331	Affected systems have been updated.
Cisco WebEx Meetings Client - On-Premises	CSCuu82694	Affected systems have been updated.
Cisco WebEx Meetings for Android	CSCuu82689	8.5 (Sept. 2015)
WebEx Meetings Server - SSL Gateway	CSCuu82699	2.6 (TBD)
WebEx Recording Playback Client	CSCuu82702	Affected systems have been updated.
Network Application, Service, and Acceleration		
Cisco ACE 30 Application Control Engine Module	CSCuu82343	Affected systems have been updated.
Cisco ACE 4710 Application Control Engine (A5)	CSCuu82343	Affected systems have been updated.
Cisco Application and Content Networking System (ACNS)	CSCuu82717	5.5.41 (Oct. 2015)
Cisco InTracer	CSCuu83316	16.4.0 (TBD)
Cisco Network Admission Control (NAC)	CSCuu83378	A patch will be available for vulnerable releases Oct. 2015.
Cisco Visual Quality Experience Server	CSCuu83371	3.10.3 (24-July-2015) 3.9.6 (31-July-2015) 3.8.7 (7-Aug-2015)
Cisco Visual Quality Experience Tools Server	CSCuu83371	3.10.3 (24-July-2015) 3.9.6 (31-July-2015) 3.8.7 (7-Aug-2015)
Cisco Wide Area Application Services (WAAS)	CSCuu82735	5.5.5 (7-Aug-2015) 6.1.0 (Sept. 2015)
Network and Content Security Devices		
Cisco ASA CX and Cisco Prime Security Manager	CSCuu82737	Affected systems will be updated 31-July-2015.
Cisco Adaptive Security Appliance (ASA)	CSCuu83280	9.2.4.1
Cisco Content Security Appliance Updater Servers	CSCuu83328	2.0.3 (TBD)
Cisco Content Security Management Appliance (SMA)	CSCuu82683	Affected systems will be updated by 30-Jun-2015.
Cisco Email Security Appliance (ESA)	CSCuu82678	TBD
Cisco FireSIGHT System Software	CSCuu82682	5.3.0.7 (14-Sept-2015) 5.3.1.6 (14-Sept-2015) 5.4.0.4 (14-Sept-2015) 5.4.1.3 (14-Sept-2015)
Cisco IPS	CSCuu82497	Cisco IPS 7.1.11 (TBD) Cisco IPS 7.3.5 (TBD)
Cisco Identity Services Engine (ISE)	CSCuu83386	1.4 (Oct 2015) 2.0 (Oct 2015)
Cisco IronPort Encryption Appliance (IEA)	CSCuu82681	No additional releases are planned.
Cisco NAC Guest Server	CSCuu82729	No additional releases are planned.
Cisco NAC Server	CSCuu82725	A patch will be available for vulnerable releases Oct. 2015.
Cisco Physical Access Control Gateway	CSCuu82476	1.5.4 (15-Aug-2015)
Cisco Secure Access Control Server (ACS)	CSCuu82493	5.008 (TBD)
Cisco Web Security Appliance (WSA)	CSCuv84060	9.0.0 (TBD)
Network Management and Provisioning		
Cisco Application Networking Manager	CSCuu82344	ANM OVA 5.2.7 (TBD)
Cisco Cloupia Unified Infrastructure Controller	CSCuu83341	5.3.2.0 (30-Jul-2015) 5.4.0.0 (30-Oct-2015)
Cisco MATE Collector	CSCuv32694	6.2.1(Aug/Sept 2015) 6.1.4 (Aug/Sept 2015)
Cisco MATE Design	CSCuv32694	6.2.1(Aug/Sept 2015) 6.1.4 (Aug/Sept 2015)
Cisco MATE Live	CSCuv32694	6.2.1(Aug/Sept 2015) 6.1.4 (Aug/Sept 2015)
Cisco Mobile Wireless Transport Manager	CSCuu83361	6.001(10-July-2015)
Cisco Multicast Manager	CSCuu82380	No additional releases are planned.

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 NewSessionTicket Double-Free Memory Corruption Vulnerability

IS OpenSSL Malformed ECParameters Infinite Loop Denial of Service Vulnerability

IS OpenSSL X509_cmp_time Read Out-of-Bounds Denial of Service Vulnerability

IS OpenSSL Missing EnvelopedContent PKCS #7 Denial of Service Vulnerability

IS OpenSSL Datagram Transport Layer Security Invalid Free Memory Corruption Vulnerability

Subscribe to Cisco Security Notifications

Subscribe

Cisco Netflow Collection Agent	CSCuu82404	1.1.1 (12-July-2015)
Cisco Network Analysis Module	CSCuu82402	6.2.1 (12-July-2015)
Cisco Packet Tracer	CSCuu82441	7.0 (24-July-2015)
Cisco Prime Access Registrar	CSCuu82382	7.0.1
Cisco Prime Collaboration Assurance	CSCuu82409	PCA 11.0 (Aug. 2015)
Cisco Prime Collaboration Deployment	CSCuu82533	11.5 (TBD)
Cisco Prime Collaboration Provisioning	CSCuu82408	11.0 (31-July-2015)
Cisco Prime Data Center Network Manager (DCNM)	CSCuu82350	Affected systems have been updated.
Cisco Prime Infrastructure Standalone Plug and Play Gateway	CSCuu83360	2.2.0.14 (July 2015)
Cisco Prime Infrastructure	CSCuu82403	3.0 (Aug. 2015)
Cisco Prime LAN Management Solution (LMS - Solaris)	CSCuu82378	4.002(005) (Aug. 2015)
Cisco Prime License Manager	CSCuu82442	11.0 (TBD)
Cisco Prime Network Registrar (CPNR)	CSCuu82381	8.1.x(TBD) 8.2.x (TBD) 8.3.2 (Sept. 2015)
Cisco Prime Network Registrar IP Address Manager (IPAM)	CSCut84576	IPAM 8.1.3 OVA
Cisco Prime Network Services Controller	CSCuu82412	Affected versions have been updated.
Cisco Prime Network	CSCuu82370	Affected systems have been updated.
Cisco Prime Optical for Service Providers	CSCuu82386	A patch will be available 25-July-2015.
Cisco Prime Performance Manager	CSCuu82372	1.6. (31-July-2015) 1.7 (Sept 2015)
Cisco Prime Security Manager	CSCuu82733	9.3.5.1 (July 2015)
Cisco Security Manager	CSCuu82411	4.7 SP2CP1 (31-July-2015) 4.8 SP1 (31-July-2015) 4.9 FCS (31-Aug-2015)
Cisco Show and Share (SnS)	CSCuu82449	5.6.1 (Aug. 2015)
Cisco UCS Central	CSCuu82364	1.4(1a) (Dec. 2015)
Local Collector Appliance (LCA)	CSCuu82760	2.2.10 (31-July-2015)
Routing and Switching - Enterprise and Service Provider		
Cisco 910 Industrial Router	CSCuu85190	1.2.1 (30-Jun-2015)
Cisco ASR 5000 Series	CSCuu83317	20.0 (TBD)
Cisco Application Policy Infrastructure Controller (APIC)	CSCuu83343	1.1(2h) 1.2(1) (pending)
Cisco Connected Grid Router - CGOS	CSCuu82349	Please migrate to NXT.
Cisco Connected Grid Router	CSCuu83373	See CSCuu82763 for fixed releases.
Cisco IOS Software and Cisco IOS XE Software	CSCuu82607	15.5(03)S (TBD)
Cisco IOS XE Software (Web UI feature only)	CSCuu82763	(TBD)
Cisco IOS XR Software	CSCuu83297	See CSCur26433 for fixed releases.
Cisco MDS 9000 Series Multilayer Switches	CSCuv71201	6.2.15 (Dec. 2015)
Cisco Nexus 1000V InterCloud	CSCuu82353	3.1.1 (TBD)
Cisco Nexus 1000V Series Switches	CSCuu82360	N1K 5.2(1)SV3(1.5) (July 2015)
Cisco Nexus 1010	CSCuu82470	5.2(1)SP1(7.4) (Oct. 2015)
Cisco Nexus 3X00 Series Switches	CSCuu82362	(TBD)
Cisco Nexus 4000 Series Blade Switches	CSCuu82499	4.1(2)E1(1p) (31-July-2015)
Cisco Nexus 5000 Series Switches	CSCuu83350	7.1(2)N1(1)
Cisco Nexus 6000 Series Switches	CSCuu83350	7.1(2)N1(1)
Cisco Nexus 7000 Series Switches	CSCuu82356	6.2.14 (15-Aug-2015) 7.2 (30-Sept-2015)
Cisco Nexus 9000 (ACI/Fabric Switch)	CSCuu83344	
Cisco Nexus 9000 Series (standalone, running NxOS)	CSCuu82359	7.0(3)I2(1).(30-Jun-2015)
Cisco ONS 15454 Series Multiservice Provisioning Platforms	CSCuu82475	10.52
Cisco OnePK All-in-One VM	CSCuu82474	Admin update via shell
Cisco Service Control Operating System	CSCuu82515	5.2.0 (Sept. 2015)
Routing and Switching - Small Business		
Cisco RV180W Wireless-N Multifunction VPN Router	CSCuu83390	No further releases are planned.
Cisco Sx220 Switches	CSCuu83388	1.1.x.x (TBD)
Cisco Sx300 Switches	CSCuu83393	1.5.x.x (June 2016)
Cisco Sx500 Switches	CSCuu83395	1.5..x.x (June 2016)
Unified Computing		
Cisco Standalone Rack Server CIMC	CSCuu82366	2.0.8 (Aug. 2015)
Cisco UCS Invicta Series Solid State Systems	CSCuu82354	TBD
Cisco Unified Computing System (Management software)	CSCuu83383	3.1(0.9)A (Oct. 2015)
Cisco Unified Computing System B-Series Blade Servers	CSCuu83352	2.2.7 (Feb. 2016)
Cisco Virtual Security Gateway	CSCuu83351	5.2(1)VSG2(1.4) (Aug. 30 2015)
Cisco Virtualization Experience Media Engine	CSCuu83434	No further releases planned.
Voice and Unified Communications Devices		
Cisco 190 ATA Series Analog Terminal Adaptor	CSCuu82526	1.2.2 (June 2016)
Cisco 8800 Series IP Phones - VPN Feature	CSCuu83429	11.0 (TBD)
Cisco ATA 187 Analog Telephone Adaptor	CSCuu82570	9.2(3) (30-Dec-2015)
Cisco Agent Desktop for Cisco Unified Contact Center Express	CSCuu83413	11.0 (Aug. 2015)
Cisco Agent Desktop	CSCuu82330	9.5(1) (TBD)
Cisco Computer Telephony Integration Object Server (CTIOS)	CSCuu82335	11.0 (TBD)
Cisco DX Series IP Phones	CSCuu82576	TBD
Cisco Emergency Responder	CSCuu82547	11.5 (TBD)
Cisco Finesse	CSCuu83416	
Cisco Hosted Collaboration Mediation Fulfillment	CSCuu82553	10.6.2 (TBD)
Cisco IM and Presence Service (CUPS)	CSCuu82551	11.5.0.98000-120 (TBD)
Cisco IP Interoperability and Collaboration System (IPICS)	CSCuu82461	IPICS 5.0 (Dec. 2015)
Cisco MediaSense	CSCuu82571	10.5 (TBD) 11.0 (TBD)
Cisco MeetingPlace	CSCuu82563	8.6 (9-July-2015)
Cisco Paging Server (InformaCast)	CSCuu82554	11.0.2 (6-July-2015)
Cisco Paging Server	CSCuu82554	11.0.2 (6-July-2015)
Cisco SPA112 2-Port Phone Adapter	CSCuu82486	1.4.1 (31-Oct-2015)
Cisco SPA122 ATA with Router	CSCuu82486	1.4.1 (31-Oct-2015)
Cisco SPA232D Multi-Line DECT ATA	CSCuu82486	1.4.1 (31-Oct-2015)
Cisco SPA30X Series IP Phones	CSCuu82490	7.6.1 (17-Sept-2015)
Cisco SPA50X Series IP Phones	CSCuu82490	7.6.1 (17-Sept-2015)
Cisco SPA51X Series IP Phones	CSCuu82490	7.6.1 (17-Sept-2015)
Cisco SPA525G	CSCuu82487	7.6.1 (17-Sept-2015)
Cisco SocialMiner	CSCuu82529	11.5(1)
Cisco Unified 7800 Series IP Phones	CSCuu82579	11.0 (Oct. 2015)
Cisco Unified 8831 Series IP Conference Phone	CSCuu82568	10.3.2 (Oct. 2015)
Cisco Unified 8945 IP Phone	CSCuu83426	TBD
Cisco Unified 8961 IP Phone	CSCuu83419	9.4(2) (Feb. 2016)
Cisco Unified 9951 IP Phone	CSCuu83419	9.4(2) (Feb. 2016)
Cisco Unified 9971 IP Phone	CSCuu83419	9.4(2) (Feb. 2016)
Cisco Unified Attendant Console Advanced	CSCuu82523	11.0.1 (19-Aug-2015)
Cisco Unified Attendant Console Business Edition	CSCuu82523	11.0.1 (19-Aug-2015)
Cisco Unified Attendant Console Department Edition	CSCuu82523	11.0.1 (19-Aug-2015)
Cisco Unified Attendant Console Enterprise Edition	CSCuu82523	11.0.1 (19-Aug-2015)
Cisco Unified Attendant Console Premium Edition	CSCuu82523	11.0.1 (19-Aug-2015)
Cisco Unified Attendant Console Standard	CSCuu82525	11.5(1) (Sept. 2015)
Cisco Unified Communications Domain Manager	CSCuu82540	Affected systems have been updated.
Cisco Unified Communications Manager (UCM)	CSCuu82530	11.5 (TBD)

Cisco Unified Communications Manager Session Management Edition (SME)	CSCuu82530	11.5 (TBD)
Cisco Unified Contact Center Enterprise	CSCuu82335	11.0 (TBD)
Cisco Unified Contact Center Express	CSCuu82538	11.0 (Aug. 2015)
Cisco Unified IP Conference Phone 8831 for Third-Party Call Control	CSCuu82519	9.3(5) (31-Dec-2015)
Cisco Unified IP Phone 7900 Series	CSCuu82580	9.4(1)SR1.2
Cisco Unified Intelligence Center (CUIC)	CSCuu82332	11.5 (May 2016)
Cisco Unified Intelligent Contact Management Enterprise	CSCuu82335	11.0 (TBD)
Cisco Unified SIP Proxy	CSCuu82329	8.5(x) (June 2016) 9.0.1 (June 2016)
Cisco Unified Wireless IP Phone	CSCuu83436	1.4.8 (Dec. 2015)
Cisco Unified Workforce Optimization	CSCuu82595	10.5 SR6 11.0
Cisco Unity Connection	CSCuu83410	9.1(2) (TBD) 11.5 (TBD) 10.5(2) (TBD)
Video, Streaming, TelePresence, and Transcoding Devices		
Cisco AnyRes Live (CAL)	CSCuu82742	9.6 (Aug. 2015)
Cisco D9036 Modular Encoding Platform	CSCuu82746	2.4 (Oct. 2015)
Cisco Digital Media Players (DMP) 4300 Series	CSCuu83362	5.4(1)RB(2P3) (15-July-2015) 5.3(6)RB(2P3) (15-July-2015)
Cisco Digital Media Players (DMP) 4400 Series	CSCuu83362	5.4(1)RB(2P3) (15-July-2015) 5.3(6)RB(2P3) (15-July-2015)
Cisco Edge 300 Digital Media Player	CSCuu82504	1.6RB3 (15-July-2015)
Cisco Edge 340 Digital Media Player	CSCuu82505	1.2 (15-July-2015)
Cisco Enterprise Content Delivery System (ECDS)	CSCuu83363	2.6.5 (31-July-2015)
Cisco Expressway Series	CSCuu82459	X8.6 (July 2015)
Cisco Headend System Release	CSCuu86854	3.0.2
Cisco Internet Streamer (CDS)	CSCuu82713	4.2 (TBD)
Cisco Jabber Video for TelePresence (Movi)	CSCuu82436	No additional releases are planned.
Cisco Media Experience Engines (MXE)	CSCuu83369	MXE3500 v3.5 (22-Jun-2015)
Cisco Media Services Interface	CSCuu82417	No additional releases are planned.
Cisco Model D9485 DAVIC QPSK	CSCuu82739	1.2.19 (31-Jul-2015)
Cisco TelePresence 1310	CSCuu82518	
Cisco TelePresence Advanced Media Gateway Series	CSCuu82419	No additional releases are planned.
Cisco TelePresence Conductor	CSCuu82420	X4.0 (27-July-2015)
Cisco TelePresence Content Server (TCS)	CSCuu74320	6.3 (21-July-2015)
Cisco TelePresence EX Series	CSCuu82450	7.3.3 (19-June-2015)
Cisco TelePresence ISDN GW 3241	CSCuu82429	2.2MR5 (Sept. 2015)
Cisco TelePresence ISDN GW MSE 8321	CSCuu82429	2.2MR5 (Sept. 2015)
Cisco TelePresence ISDN Link	CSCuu82431	1.1.6 (Jan. 2016)
Cisco TelePresence MCU (8510, 8420, 4200, 4500 and 5300)	CSCuu82435	4.5MR2 (July 2015)
Cisco TelePresence MX Series	CSCuu82450	7.3.3 (19-June-2015)
Cisco TelePresence Profile Series	CSCuu82450	7.3.3 (19-June-2015)
Cisco TelePresence SX Series	CSCuu82450	7.3.3 (19-June-2015)
Cisco TelePresence Serial Gateway Series	CSCuu82447	1.0MR5 (Oct. 2015)
Cisco TelePresence Server 8710, 7010	CSCuu82452	4.2 (July 2015)
Cisco TelePresence Server on Multiparty Media 310, 320	CSCuu82452	4.2 (July 2015)
Cisco TelePresence Server on Virtual Machine	CSCuu82452	4.2 (July 2015)
Cisco TelePresence Supervisor MSE 8050	CSCuu82437	2.3 (July 2015)
Cisco TelePresence System 1000	CSCuu82518	
Cisco TelePresence System 1100	CSCuu82518	
Cisco TelePresence System 1300	CSCuu82518	
Cisco TelePresence System 3000 Series	CSCuu82518	
Cisco TelePresence System 500-32	CSCuu82518	
Cisco TelePresence System 500-37	CSCuu82518	
Cisco TelePresence TX 9000 Series	CSCuu82518	
Cisco TelePresence Video Communication Server (VCS)	CSCuu82459	X8.6 (July 2015)
Cisco Telepresence Integrator C Series	CSCuu82450	7.3.3 (19-June-2015)
Cisco VEN501 Wireless Access Point	CSCuu82710	20.2.48.11 (July 2015)
Cisco Video Distribution Suite for Internet Streaming (VDS-IS/CDS-IS)	CSCuu83370	4.2 (31-July-2015)
Cisco Video Surveillance 3000 Series IP Cameras	CSCuu82480	2.7 (31-Jan-2016)
Cisco Video Surveillance 4000 Series High-Definition IP Cameras	CSCuu82478	Affected systems will be updated 31-Jan-2016.
Cisco Video Surveillance 4300E/4500E High-Definition IP Cameras	CSCuu82479	Affected systems will be updated 31-Jan-2016.
Cisco Video Surveillance 6000 Series IP Cameras	CSCuu82480	2.7 (31-Jan-2016)
Cisco Video Surveillance 7000 Series IP Cameras	CSCuu82480	2.7 (31-Jan-2016)
Cisco Video Surveillance Media Server	CSCuu82481	7.7.0 (26-Sept-2015)
Cisco Video Surveillance PTZ IP Cameras	CSCuu82480	2.7 (31-Jan-2016)
Cisco Videoscape Control Suite	CSCuu86705	3.6 (TBD)
Cloud Object Store (COS)	CSCuu82712	2.1.2 (Available) 3.0.1 (24-July-2015)
Tandberg Codian ISDN GW 3210/3220/3240	CSCuu82429	2.2MR5 (Sept. 2015)
Tandberg Codian MSE 8320 Model	CSCuu82429	2.2MR5 (Sept. 2015)
Wireless		
Cisco IOS Access Points	CSCuu71585	See CSCuu82607 for first fixes.
Cisco Mobility Services Engine (MSE)	CSCuu83358	8.0 - 8.0.130.0 (15-Oct-2015)
Cisco Wireless LAN Controller (WLC)	CSCuu82416	8.2 and previous releases (Nov. 2015)
Cisco Hosted Services		
Cisco Common Services Platform Collector	CSCuu82668	Affected systems have been updated.
Cisco Connected Analytics For Collaboration	CSCuu82671	A patch will be available June 30, 2015.
Cisco Intelligent Automation for Cloud	CSCuu82460	A patch file is available for vulnerable releases.
Cisco Registered Envelope Service (CRES)	CSCuu83326	4.4.1 (10-Jun-2015)
Cisco Universal Small Cell 5000 Series running V3.4.2.x software	CSCuu82508	V3.4.2.24 (July 2015)
Cisco Universal Small Cell 7000 Series running V3.4.2.x software	CSCuu82508	V3.4.2.24 (July 2015)
Cisco Universal Small Cell CloudBase	CSCuu83403	TBD
Cisco WebEx Messenger Service	CSCuu82700	7.9.8 EP 1 (19-Jun-2015)
Cisco Webex Multimedia Platform	CSCuu83333	3.8.3.1
Partner Supporting Service (PSS) 1.x	CSCuu83380	2.7 (10-Jul-2015)
Small Cell factory recovery root filesystem V2.99.4 or later	CSCuu83402	TBD

Products Confirmed Not Vulnerable

Cisco has confirmed that the following products are not vulnerable to the six distinct vulnerabilities announced by the OpenSSL Project on June 11, 2015:

Endpoint Clients and Client Software

- Cisco IP Communicator
- 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 for BlackBerry
- Cisco WebEx Productivity Tools

Network Application, Service, and Acceleration

- Cisco ACE GSS 4400 Series Global Site Selector
- Cisco CSS 11500 Series Content Security Switch
- Cisco Extensible Network Controller (XNC)
- Cisco Nexus Data Broker (NDB)

Network and Content Security Devices

- Cisco ASA Content Security and Control (CSC) Security Services Module
- Cisco Adaptive Security Device Manager
- Cisco Physical Access Manager

Network Management and Provisioning

- Cisco Configuration Professional
- Cisco Connected Grid Device Manager
- Cisco Connected Grid Network Management System
- Cisco Insight Reporter
- Cisco Linear Stream Manager
- Cisco MGC Node Manager (CMNM)
- Cisco Prime Analytics
- Cisco Prime Cable Provisioning
- Cisco Prime Central for SPs
- Cisco Prime Collaboration Manager
- Cisco Prime Home
- Cisco Prime Provisioning for SPs
- Cisco Prime Provisioning
- Cisco Unified Provisioning Manager (CUPM)
- CiscoWorks Network Compliance Manager

Routing and Switching - Enterprise and Service Provider

- Cisco Broadband Access Center Telco Wireless
- Cisco IOS XE Software (SSL VPN feature)

Voice and Unified Communications Devices

- Cisco 7937 IP Phone
- Cisco Billing and Measurements Server
- Cisco PSTN Gateway (PGW) 2200
- Cisco Packaged Contact Center Enterprise
- Cisco Remote Silent Monitoring
- 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 6900 Series IP Phones
- Cisco Unified 6901 IP Phones
- Cisco Unified 6911 IP Phones
- Cisco Unified 6945 IP Phones
- Cisco Unified Client Services Framework
- Cisco Unified E-Mail Interaction Manager
- Cisco Unified Integration for IBM Sametime
- Cisco Unified Operations Manager (CUOM)
- Cisco Unified Web Interaction Manager
- Cisco Voice Portal (CVP)
- Exony VIM/CCDM/CCMP

Video, Streaming, TelePresence, and Transcoding Devices

- Cisco AnyRes VOD (CAL)
- Cisco D9034-S Encoder
- Cisco D9054 HDTV Encoder
- Cisco D9804 Multiple Transport Receiver
- 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 TelePresence Exchange System (CTX)
- 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 Virtual PGW 2200 Softswitch

Wireless

- Cisco Wireless Control System (WCS)

Cisco Hosted Services

- Cisco Cloud Web Security
- Cisco Communication/Collaboration Sizing Tool
- Cisco Unified Communications Upgrade Readiness Assessment
- Cisco Unified Services Delivery Platform (CUSDP)
- Cisco Virtual Machine Placement Tool
- Cisco WebEx Meetings (Meeting Center, Training Center, Event Center, Support Center)
- Cisco WebEx WebOffice Workspace

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

The OpenSSL Project disclosed six vulnerabilities and a protection against Diffie-Hellman (DH) on June 11, 2015. One or more of these vulnerabilities affect both client and server installations of OpenSSL. The vulnerability names and the associated Common Vulnerabilities and Exposures (CVE) IDs are as follows.

The impact of these vulnerabilities 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.

DHE Man-in-the-Middle Protection (Logjam)

OpenSSL has added protection for Transport Layer Security (TLS) clients by rejecting handshakes with DH parameters shorter than 768 bits. Previously, Cisco published a blog regarding the DHE man-in-the-middle attack (Logjam) at the following location Understanding Logjam and Future-Proofing Your Infrastructure**.**

OpenSSL X509_cmp_time Read Out-of-Bounds Denial of Service Vulnerability

A vulnerability in OpenSSL could allow an unauthenticated, remote attacker to cause a denial of service(DoS) condition on a targeted system.

The vulnerability is due to improper bounds checks being done on user-supplied input by the affected software. An attacker could exploit this vulnerability by submitting crafted certificates and certificate revocation lists (CRLs) to be processed by the affected software. A successful exploit could allow the attacker to cause a DoS condition on the system.

This vulnerability has been assigned CVE ID CVE-2015-1789.

OpenSSL CMS Verify Unknown Hash Function Denial of Service Vulnerability

A vulnerability in OpenSSL could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

The vulnerability is due to improper processing of user-supplied input by the affected software. An unauthenticated, remote attacker could exploit the vulnerability by transmitting crafted messages to the targeted system. Processing such messages could allow the attacker to cause the affected software to stop responding. A successful exploit could allow the attacker to cause a DoS condition on the targeted system.

This vulnerability has been assigned CVE ID CVE-2015-1792.

OpenSSL DTLS Invalid Free Memory Corruption Vulnerability

OpenSSL contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on a targeted system.

The vulnerability is due to insufficient validation of the Datagram Transport Layer Security (DTLS) peer data. An unauthenticated, remote attacker could exploit the vulnerability by submitting crafted application data to the affected software. A successful exploit could allow the attacker to cause a DoS condition, denying service to legitimate users.

This vulnerability has been assigned CVE ID CVE-2014-8176.

OpenSSL Malformed ECParameters Infinite Loop Denial of Service Vulnerability

A vulnerability in OpenSSL could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

The vulnerability is due to improper processing of user-supplied input. An attacker could exploit the vulnerability by transmitting crafted requests to the targeted system. Processing such requests could allow the attacker to cause the affected software to stop responding.

This vulnerability has been assigned CVE ID CVE-2015-1788.

OpenSSL Missing EnvelopedContent PKCS #7 Denial of Service Vulnerability

A vulnerability in OpenSSL could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

The vulnerability exists because the affected software improperly handles user-supplied Public-Key Cryptography Standard #7 (PKCS #7) data. An attacker could exploit the vulnerability by transmitting a crafted request to the targeted system. Processing the request could cause the affected software to stop responding and cause a DoS condition for legitimate users.

This vulnerability has been assigned CVE ID CVE-2015-1790.

OpenSSL NewSessionTicket Double-Free Memory Corruption Vulnerability

A vulnerability in OpenSSL could allow an unauthenticated, remote attacker to cause memory corruption errors.

The vulnerability exists because the affected software improperly handles session data. An attacker could exploit the vulnerability by transmitting crafted session requests to the targeted system. When processing such requests the affected software may cause memory corruption errors and could cause a denial of service (DoS) condition.

This vulnerability has been assigned CVE ID CVE-2015-1791.

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 and Responses 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 vulnerabilities that are described in this advisory.

These vulnerabilities were publicly disclosed by the OpenSSL Project on June 11, 2015.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150612-openssl

---

Revision History

Version	Description	Section	Status	Date
1.17	Updated the first fixed release information for Cisco SocialMiner.	Affected Products	Final	2017-January-17
1.16	Updated first fixed software for APIC from 1.2(1) (Sept. 2015) to 1.1(2h), 1.2(1) (pending). Updated first fixed software for Cisco Nexus 9000 (ACI/Fabric Switch) from Affected systems have been updated to 11.1(2)	Affected Products	Final	2015-November-13
1.15	Cisco Unified Computing System B-Series (Blade) Servers had the first fixed software updated to 2.2.7 (February 2016).	Affected Products		2015-November-04
1.14	Updated Cisco MDS 9000 Series Multilayer Switches to point to a new bug ID and removed the first fixed version of 5.2.8h (Mar 2016). Updated the bug ID for Cisco Web Security Appliance (WSA).	Affected Products		2015-October-16
1.13	Cisco Unified Intelligence Center (CUIC) first fixed was changed from 11.0 (Aug 2015) to 11.5 (May 2016).	Affected Products		2015-October-07
1.12	Updated Affected Products section.			2015-August-24
1.11	Updated Affected Products section.			2015-July-30
1.10	Updated Affected Products section.			2015-July-24
1.9	Updated Affected Products section. Updated bug IDs for Nexus products.			2015-July-16
1.8	Updated Affected Products section.			2015-July-15
1.7	Updated Affected Products section.			2015-July-09
1.6	Updated Affected Products section.			2015-July-07
1.5	Updated Affected Products section.			2015-July-06
1.4	Updated Affected Products section.			2015-June-23
1.3	Updated Affected Products section.			2015-June-19
1.2	Updated Affected Products section.			2015-June-17
1.1	Updated Affected Products section.			2015-June-16
1.0	Initial public release.			2015-June-12
