Cisco Security Advisory

Multiple Vulnerabilities in OpenSSL (December 2015) Affecting Cisco Products

Advisory ID: cisco-sa-20151204-openssl
Last Updated: 2016 September 21 22:47 GMT
Published: 2015 December 4 17:38 GMT
Version1.12: Final
Workarounds: No workarounds available

CVE-2015-1794
CVE-2015-3193
CVE-2015-3194
CVE-2015-3195
CVE-2015-3196
CWE-399

Download CVRF
Download PDF
Email

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 BN_mod_exp Function Security Bypass Vulnerability

IS OpenSSL Anonymous Diffie-Hellman Cipher Suite Processing Denial of Service Vulnerability

ST 37154

ST 37155

Subscribe to Cisco Security Notifications

Subscribe

Summary

On December 3, 2015, the OpenSSL Project released a security advisory detailing five vulnerabilities.

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.

This advisory will be updated as additional information becomes available.

Cisco will release software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are not available.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151204-openssl

Affected Products

Cisco has completed its investigation to its product line to determine which products may be affected by these vulnerabilities and the impact on each affected product. 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 five vulnerabilities in the December 3, 2015, OpenSSL Project security advisory:

Product	Defect	Fixed releases availability
Collaboration and Social Media		
Cisco SocialMiner	CSCux41444	
Cisco WebEx Meetings Server versions 1.x	CSCux41312	2.5MR6 (Available) 2.6MR1 (28-Jan-2016)
Cisco WebEx Meetings Server versions 2.x	CSCux41312	2.5MR6 (Available) 2.6MR1 (28-Jan-2016)
Cisco WebEx Node for MCS	CSCux41308	3.12.9.7
Endpoint Clients and Client Software		
Cisco Agent for OpenFlow	CSCux41418	2.0.4-r3 (Jan 2016) 2.0.3-r1 (Jan 2016) 2.1.3-r1 (Jan 2016) 1.1.4-r2 (Jan 2016
Cisco AnyConnect Secure Mobility Client for Android	CSCux41420	Windows: 3.1.13011 (Available) Windows: 4.2.x (Dec 2016) OS X: 3.1.13011 (Available) OS X: 4.2.x (Dec 2016) Linux: 3.1.13011 (Available) Linux: 4.2.x (Dec 2016) Android: 4.0.x (Jan 2016) iOS 4.0.x (Jan 2016)
Cisco AnyConnect Secure Mobility Client for Linux	CSCux41420	Windows: 3.1.13011 (Available) Windows: 4.2.x (Dec 2016) OS X: 3.1.13011 (Available) OS X: 4.2.x (Dec 2016) Linux: 3.1.13011 (Available) Linux: 4.2.x (Dec 2016) Android: 4.0.x (Jan 2016) iOS 4.0.x (Jan 2016)
Cisco AnyConnect Secure Mobility Client for OS X	CSCux41420	Windows: 3.1.13011 (Available) Windows: 4.2.x (Dec 2016) OS X: 3.1.13011 (Available) OS X: 4.2.x (Dec 2016) Linux: 3.1.13011 (Available) Linux: 4.2.x (Dec 2016) Android: 4.0.x (Jan 2016) iOS 4.0.x (Jan 2016)
Cisco AnyConnect Secure Mobility Client for Windows	CSCux41420	Windows: 3.1.13011 (Available) Windows: 4.2.x (Dec 2016) OS X: 3.1.13011 (Available) OS X: 4.2.x (Dec 2016) Linux: 3.1.13011 (Available) Linux: 4.2.x (Dec 2016) Android: 4.0.x (Jan 2016) iOS 4.0.x (Jan 2016)
Cisco AnyConnect Secure Mobility Client for iOS	CSCux41420	Windows: 3.1.13011 (Available) Windows: 4.2.x (Dec 2016) OS X: 3.1.13011 (Available) OS X: 4.2.x (Dec 2016) Linux: 3.1.13011 (Available) Linux: 4.2.x (Dec 2016) Android: 4.0.x (Jan 2016) iOS 4.0.x (Jan 2016)
Cisco Jabber Guest 10.0(2)	CSCux67343	10.6.10 (5-Feb-2015)
Cisco Jabber Software Development Kit	CSCux41459	11.0.1 (28-Jan-2016)
Cisco Jabber for Android	CSCux41478	11.5.1 (31-Jan-2016)
Cisco Jabber for Mac	CSCux41458	11.5.1 (Feb 2016)
Cisco Jabber for Windows	CSCux41461	11.1.3 (13-Jan-2016) 10.6.7 (26-Jan-2016) 11.5.1 (9-Feb-2016
Cisco Jabber for iOS	CSCux41457	
Cisco WebEx Meetings Client - Hosted	CSCux41316	T31R1 (31-Mar-2016) T30SP5 (Feb 2016)
Cisco WebEx Meetings Client - On Premises	CSCux41311	2.6MR1 (28-Jan-2016)
Cisco WebEx Meetings for Android	CSCux41309	8.6 (22-Dec-2015)
Cisco WebEx Meetings for WP8	CSCux41310	2.6 (15-Jan-2016)
WebEx Meetings Server - SSL Gateway	CSCux41313	2.5MR6 (Available) 2.6MR1 (28-Jan-2016)
WebEx Recording Playback Client	CSCux41315	T31R1 (Available) T31R1 (Available) ER 9 (Jan 2016) BTS (Feb 2016) LA (Mar 2016) GA (April 2016)
Network Application, Service, and Acceleration		
Cisco InTracer	CSCux41293	No plan to release a new ISO image of the kernel. Admin to update package via CLI.
Cisco Network Admission Control (NAC)	CSCux41386	0.9.8zh (30-Jan-2016)
Cisco Visual Quality Experience Server	CSCux41384	3.10 (TBD)
Cisco Visual Quality Experience Tools Server	CSCux41384	3.10 (TBD)
Cisco Wide Area Application Services (WAAS)	CSCux41499	
Network and Content Security Devices		
Cisco ASA CX and Cisco Prime Security Manager	CSCux41395	MR7 (Feb 2016)

Cisco ASA Next-Generation Firewall Services	CSCux41393	
Cisco Adaptive Security Appliance (ASA)	CSCux41145	9.1.7 (Jan 2016)
Cisco Clean Access Manager	CSCux41388	0.9.8zh (30-Jan-2016)
Cisco Content Security Management Appliance (SMA)	CSCux41305	10.0 (May 2016)
Cisco Email Security Appliance (ESA)	CSCux41303	10.0.0 (5-Apr-2016)
Cisco FireSIGHT System Software	CSCux41304	
Cisco IPS	CSCux41422	7.3(05) Patch 1 (Mar 2016) 7.1(11) Patch 1 (Mar 2016)
Cisco Identity Services Engine (ISE)	CSCux41407	
Cisco NAC Guest Server	CSCux56314	Patch updates available (30-Jan-2016)
Cisco NAC Server	CSCux41389	0.9.8zh (30-Jan-2016)
Cisco Physical Access Control Gateway	CSCux41401	5.4.2 (21-Feb-2016)
Cisco Virtual Security Gateway for Microsoft Hyper-V	CSCux41332	5.2(1)VSG2(1.5) (30-May-2016)
Cisco Web Security Appliance (WSA)	CSCux41307	10.5 (Nov 2016)
Network Management and Provisioning		
Cisco Netflow Collection Agent	CSCux41348	Patch update available (4-Jan-2016) 1.1.2 (1-Jul-2016)
Cisco Network Analysis Module	CSCux41345	6.3.1 (Mar 2016)
Cisco Packet Tracer	CSCux41366	7.0 (29-Jul-2015)
Cisco Prime Access Registrar	CSCux41341	7.1.0.4 (11-Jan-2016)
Cisco Prime Collaboration Assurance	CSCux41350	11.1 (Feb 2016)
Cisco Prime Collaboration Deployment	CSCux41446	11.5.0 (June 2016)
Cisco Prime Collaboration Provisioning	CSCux41349	11.1 (22-Feb-2016)
Cisco Prime Data Center Network Manager (DCNM)	CSCux41321	7.2(3) (29-Jan-2016)
Cisco Prime IP Express	CSCux41343	
Cisco Prime Infrastructure	CSCux41347	
Cisco Prime License Manager	CSCux41367	11.5.0 (June 2016)
Cisco Prime Network Registrar (CPNR)	CSCux41340	8.3.4 (Feb 2016) 8.2.4 (Feb 2016) 8.1.4 (Feb 2016)
Cisco Prime Network Registrar IP Address Manager (IPAM)	CSCux41536	8.3 (Jul 2016)
Cisco Prime Network	CSCux41336	PN423 (Mar 2016)
Cisco Prime Optical for SPs	CSCux41342	10.6 (30-Jun-2016)
Cisco Prime Performance Manager	CSCux41337	PPM 1.7 SP3 (Feb 2016)
Cisco Quantum Policy Suite (QPS)	CSCux41565	9.0 (18-Mar-2016)
Cisco Security Manager	CSCux41352	4.10 (23-Dec-2015) 4.9 SP1CP1 (18-Dec-2015) 4.8 SP1CP2 (Jan 2016)
Cisco Show and Share (SnS)	CSCux41370	5.6.2 (31-May-2016)
Cisco UCS Central	CSCux41334	1.5(1a) (July 2016)
Local Collector Appliance (LCA)	CSCux41433	2.2.11 (Jan 2016)
Routing and Switching - Enterprise and Service Provider		
Cisco ASR 5000 Series	CSCux41294	
Cisco Application Policy Infrastructure Controller (APIC)	CSCux41322	Maintenance Release (1.2(2) (Feb 2016)
Cisco MDS 9000 Series Multilayer Switches	CSCux41326	7.3 MR
Cisco Nexus 1000V InterCloud	CSCux41324	2.3 (Jun 2016)
Cisco Nexus 1000V Series Switches	CSCux41328	5.2(1)SV3(1.11) (16-Feb-2016)
Cisco Nexus 3X00 Series Switches	CSCux41329	
Cisco Nexus 4000 Series Blade Switches	CSCux41423	4.1(2)E1(1q) (Jun 2016)
Cisco Nexus 5000 Series Switches	CSCux41326	7.3 MR
Cisco Nexus 5000 Series Switches	CSCux41330	
Cisco Nexus 6000 Series Switches	CSCux41326	7.3 MR
Cisco Nexus 7000 Series Switches	CSCux41326	7.3 MR
Cisco Nexus 9000 (ACI/Fabric Switch)	CSCux41323	
Cisco Nexus 9000 Series (standalone, running NxOS)	CSCux41327	7.0(3)I3(1) (15-Jan-2016)
Cisco ONS 15454 Series Multiservice Provisioning Platforms	CSCux41400	10.5.2 (TBD)
Routing and Switching - Small Business		
Cisco Sx220 switches	CSCux41409	Version TBD maintenance release scheduled Mar 2016
Unified Computing		
Cisco Standalone rack server CIMC	CSCux41335	2.0(11) (31-May-2016)
Cisco Unified Computing System (Management software)	CSCux41399	
Cisco Unified Computing System B-Series (Blade) Servers	CSCux41398	3.1(20) (Feb 2016)
Cisco Virtual Security Gateway	CSCux41331	5.2(1)VSG2(1.5) (30-May-2016)
Voice and Unified Communications Devices		
Cisco 190 ATA Series Analog Terminal Adaptor	CSCux41443	1.2.2 (30-Jun-2016)
Cisco 8800 Series IP Phones - VPN Feature	CSCux41472	11.5(1) (31-Mar-2016)
Cisco ATA 187 Analog Telephone Adaptor	CSCux41467	9.2.3.1-es13 (15-Apr-2016)
Cisco Agent Desktop for Cisco Unified Contact Center Express	CSCux41449	
Cisco Agent Desktop	CSCux41300	
Cisco Emergency Responder	CSCux41451	11.5 (June 2016)
Cisco Finesse	CSCux41554	11.5.1 (Release Date TBD)
Cisco Hosted Collaboration Mediation Fulfillment	CSCux41455	10.6.3 (23-Dec-2015)
Cisco IM and Presence Service (CUPS)	CSCux41453	10.5.2 (Feb 2016)
Cisco IP Interoperability and Collaboration System (IPICS)	CSCux41377	5.0(1) (April 2016)
Cisco MediaSense	CSCux41468	11.5.1 (31-May-2016)
Cisco MeetingPlace	CSCux41463	8.6 MR1 (5-Feb-2016)
Cisco SPA112 2-Port Phone Adapter	CSCux41410	1.4.2 (30-June-2016)
Cisco SPA122 ATA with Router	CSCux41410	1.4.2 (30-June-2016)
Cisco SPA232D Multi-Line DECT ATA	CSCux41410	1.4.2 (30-June-2016)
Cisco SPA525G	CSCux41411	7.6.2 (15-Apr-2016)
Cisco Unified 7800 Series IP Phones	CSCux41473	10.5.1 (Mar 2016)
Cisco Unified 8831 series IP Conference Phone	CSCux41465	10.3.1SR3 (TBD)
Cisco Unified 8945 IP Phone	CSCux41464	9.4.2SR3 (TBD)
Cisco Unified Attendant Console Advanced	CSCux41440	11.5.1 (30-Sep-2016)
Cisco Unified Attendant Console Business Edition	CSCux41440	11.5.1 (30-Sep-2016)
Cisco Unified Attendant Console Department Edition	CSCux41440	11.5.1 (30-Sep-2016)
Cisco Unified Attendant Console Enterprise Edition	CSCux41440	11.5.1 (30-Sep-2016)
Cisco Unified Attendant Console Premium Edition	CSCux41440	11.5.1 (30-Sep-2016)
Cisco Unified Attendant Console Standard	CSCux41442	11.5.1 (30-Sep-2016)
Cisco Unified Communications Domain Manager	CSCux41450	11.5.1 (30-Apr-2016)
Cisco Unified Communications Manager (UCM)	CSCux41445	11.5.0 (June 2016)
Cisco Unified Communications Manager Session Management Edition (SME)	CSCux41445	11.5.0 (June 2016)
Cisco Unified Contact Center Express	CSCux41545	11.5.1 (TBD)
Cisco Unified IP Conference Phone 8831 for Third-Party Call Control	CSCux41439	9.3.5 (30-Aug-2016)
Cisco Unified Intelligence Center (CUIC)	CSCux41548	11.5(1) (6-Jun-2016)
Cisco Unified Workforce Optimization	CSCux41481	

Cisco Unity Connection	CSCux41447	11.5.0 (June 2016)
Cisco Virtualization Experience Media Engine	CSCux41480	11.5.1 (28-Jan-2016)
Video, Streaming, TelePresence, and Transcoding Devices		
Cisco AnyRes Live (CAL)	CSCux41430	9.6.2 (21-Dec-2015)
Cisco Digital Media Players (DMP) 4300 Series	CSCux41357	5.3(6)RB(2P4) 10-Jan-2016 5.4(1)RB(2P6) 10-Jan-2016
Cisco Digital Media Players (DMP) 4400 Series	CSCux41357	5.3(6)RB(2P4) 10-Jan-2016 5.4(1)RB(2P6) 10-Jan-2016
Cisco Edge 300 Digital Media Player	CSCux41425	1.6RB4_3 (8-Jan-2016)
Cisco Edge 340 Digital Media Player	CSCux41426	A patch file will be available by 18-Jan-2016.
Cisco Enterprise Content Delivery System (ECDS)	CSCux41358	2.6.6 (Jan 2016)
Cisco Expressway Series	CSCux41206	X8.7.1 (Feb 2016)
Cisco Internet Streamer (CDS)	CSCux41383	4.3 (Feb 2016)
Cisco Media Experience Engines (MXE)	CSCux41365	A patch file will be available for 3.5 by 18-Dec-2015.
Cisco Model D9485 DAVIC QPSK	CSCux41429	Update scheduled for 27-Feb-2016
Cisco TelePresence 1310	CSCux41438	Next Fixed Release (Jan 2016)
Cisco TelePresence Advanced Media Gateway Series	CSCux41355	Product has reached End of Software Maintenance no further releases are forthcoming.
Cisco TelePresence Conductor	CSCux41356	XC4.2 (29-Feb-2016)
Cisco TelePresence Content Server (TCS)	CSCux41372	7.1 (April 2016)
Cisco TelePresence EX Series	CSCux41371	6.3.5 (31-Jan-2016) 7.3.5 (25-Mar-2016) 8.1.0 (25-Mar-2016)
Cisco TelePresence ISDN GW 3241	CSCux41360	2.2(1.112) (Jun 2016)
Cisco TelePresence ISDN GW MSE 8321	CSCux41360	2.2(1.112) (Jun 2016)
Cisco TelePresence ISDN Link	CSCux41361	1.1.5 (Available) 1.1.6 (8-Jan-2016)
Cisco TelePresence MCU (8510, 8420, 4200, 4500 and 5300)	CSCux41362	4.5(1.85) (Apr 2016)
Cisco TelePresence MX Series	CSCux41371	6.3.5 (31-Jan-2016) 7.3.5 (25-Mar-2016) 8.1.0 (25-Mar-2016)
Cisco TelePresence Profile Series	CSCux41371	6.3.5 (31-Jan-2016) 7.3.5 (25-Mar-2016) 8.1.0 (25-Mar-2016)
Cisco TelePresence SX Series	CSCux41371	6.3.5 (31-Jan-2016) 7.3.5 (25-Mar-2016) 8.1.0 (25-Mar-2016)
Cisco TelePresence Serial Gateway Series	CSCux41368	1.0(1.49) (Jul 2016)
Cisco TelePresence Server 8710, 7010	CSCux41374	4.3 (9-Feb-2016)
Cisco TelePresence Server on Multiparty Media 310, 320	CSCux41374	4.3 (9-Feb-2016)
Cisco TelePresence Server on Virtual Machine	CSCux41374	4.3 (9-Feb-2016)
Cisco TelePresence Supervisor MSE 8050	CSCux41364	2.3(1.47) (May 2016)
Cisco TelePresence System 1000	CSCux41438	Next Fixed Release (Jan 2016)
Cisco TelePresence System 1100	CSCux41438	Next Fixed Release (Jan 2016)
Cisco TelePresence System 1300	CSCux41438	Next Fixed Release (Jan 2016)
Cisco TelePresence System 3000 Series	CSCux41438	Next Fixed Release (Jan 2016)
Cisco TelePresence System 500-32	CSCux41438	Next Fixed Release (Jan 2016)
Cisco TelePresence System 500-37	CSCux41438	Next Fixed Release (Jan 2016)
Cisco TelePresence TX 9000 Series	CSCux41438	Next Fixed Release (Jan 2016)
Cisco TelePresence Video Communication Server (VCS)	CSCux41206	X8.7.1 (Feb 2016)
Cisco Telepresence Integrator C Series	CSCux41371	6.3.5 (31-Jan-2016) 7.3.5 (25-Mar-2016) 8.1.0 (25-Mar-2016)
Cisco VEN501 Wireless Access Point	CSCux41378	
Cisco Video Distribution Suite for Internet Streaming (VDS-IS/CDS-IS)	CSCux41382	4.3 (Feb 2016)
Cisco Video Surveillance 3000 Series IP Cameras	CSCux41404	2.8 (0.20) (4-Mar-2016)
Cisco Video Surveillance 3000 Series IP Cameras	CSCux41405	2.8 (0.20) (4-Mar-2016)
Cisco Video Surveillance 4000 Series High-Definition IP Cameras	CSCux41402	2.4.7 (4-Mar-2016)
Cisco Video Surveillance 4300E/4500E High-Definition IP Cameras	CSCux41403	3.2.8 (4-Mar-2016)
Cisco Video Surveillance 6000 Series IP Cameras	CSCux41404	2.8 (0.20) (4-Mar-2016)
Cisco Video Surveillance 6000 Series IP Cameras	CSCux41405	2.8 (0.20) (4-Mar-2016)
Cisco Video Surveillance 7000 Series IP Cameras	CSCux41404	2.8 (0.20) (4-Mar-2016)
Cisco Video Surveillance 7000 Series IP Cameras	CSCux41405	2.8 (0.20) (4-Mar-2016)
Cisco Video Surveillance PTZ IP Cameras	CSCux41404	2.8 (0.20) (4-Mar-2016)
Cisco Video Surveillance PTZ IP Cameras	CSCux41405	2.8 (0.20) (4-Mar-2016)
Cisco Videoscape Control Suite	CSCux41379	3.5.3 (29-Feb-2016) 3.6 (29-Feb-2016) 4.0 (29-Feb-2016)
Tandberg Codian ISDN GW 3210/3220/3240	CSCux41360	2.2(1.112) (Jun 2016)
Tandberg Codian MSE 8320 model	CSCux41360	2.2(1.112) (Jun 2016)
Wireless		
Cisco Mobility Services Engine (MSE)	CSCux41344	
Cisco Wireless LAN Controller (WLC)	CSCux41354	8.0 MR3 (2016) 8.1 MR (Feb 2016) 8.2 MR1 (2016) 8.3 (Apr 2016)
Cisco Hosted Services		
Cisco Cloud Web Security	CSCux41551	Update available June 2016.
Cisco Connected Analytics For Collaboration	CSCux41297	1.6 (31-Mar-2016)
Cisco Registered Envelope Service (CRES)	CSCux41302	4.5.1 (16-Jan-2015)
Cisco Universal Small Cell 5000 Series running V3.4.2.x software	CSCux41427	3.4 (29-Feb-2016) 3.5 (31-Jan-2016)
Cisco Universal Small Cell 7000 Series running V3.4.2.x software	CSCux41427	3.4 (29-Feb-2016) 3.5 (31-Jan-2016)
Cisco WebEx Messenger Service	CSCux41314	7.14.2 (14-Dec-2015)
Cisco Webex Multimedia Platform	CSCux41317	3.9 (15-Jan-2016)
Services Analytic Platform	CSCux41298	1.6 (31-Mar-2016)
Small Cell factory recovery root filesystem V2.99.4 or later	CSCux41533	3.4.4.10 (29-Feb-2016) 3.5.12.16 (31-Jan-2016)

Products Confirmed Not Vulnerable

Cisco has confirmed that the following products are not vulnerable to the five vulnerabilities announced by the OpenSSL Project on December 3, 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 WebEx Meetings for BlackBerry
- Cisco WebEx Productivity Tools

Network Application, Service, and Acceleration

- Cisco ACE 30 Application Control Engine Module
- Cisco ACE 4710 Application Control Engine (A5)
- Cisco Application and Content Networking System (ACNS)
- 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 Content Security Appliance Updater Servers
- Cisco Physical Access Manager
- Cisco Secure Access Control Server (ACS)

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 Insight Reporter
- Cisco Linear Stream Manager
- Cisco MATE Collector
- Cisco MATE Design
- Cisco MATE Live
- Cisco MGC Node Manager (CMNM)
- Cisco Mobile Wireless Transport Manager
- Cisco Prime Analytics
- Cisco Prime Cable Provisioning
- Cisco Prime Central for SPs
- Cisco Prime Collaboration Manager
- Cisco Prime Home
- Cisco Prime Infrastructure Standalone Plug and Play Gateway
- Cisco Prime LAN Management Solution (LMS - Solaris)
- 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 910 Industrial Router
- Cisco IOS Software and Cisco IOS-XE Software
- Cisco IOS-XE (SSLVPN feature)
- Cisco IOS-XE (WebUI feature only)
- Cisco IOS-XR
- Cisco Nexus 1010
- Cisco Service Control Operating System

Routing and Switching - Small Business

- Cisco Sx300 switches
- Cisco Sx500 switches
- Cisco sx20xx_xx switches

Unified Computing

- Cisco Common Services Platform Collector
- Cisco UCS Invicta Series Solid State Systems

Voice and Unified Communications Devices

- Cisco 7937 IP Phone
- Cisco Billing and Measurements Server
- Cisco Computer Telephony Integration Object Server (CTIOS)
- Cisco DX Series IP Phones
- Cisco Packaged Contact Center Enterprise
- Cisco Paging Server (Informacast)
- Cisco Paging Server
- Cisco Remote Silent Monitoring
- Cisco SPA30X Series IP Phones
- Cisco SPA50X Series IP Phones
- Cisco SPA51X Series IP Phones
- 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 6921 IP Phones
- Cisco Unified 6945 IP Phones
- Cisco Unified 8961 IP Phone
- Cisco Unified 9951 IP Phone
- Cisco Unified 9971 IP Phone
- Cisco Unified Client Services Framework
- Cisco Unified Contact Center Enterprise
- Cisco Unified E-Mail Interaction Manager
- Cisco Unified IP Phone 7900 Series
- Cisco Unified Intelligent Contact Management Enterprise
- Cisco Unified Operations Manager (CUOM)
- Cisco Unified Sip Proxy
- Cisco Unified Web Interaction Manager
- Cisco Unified Wireless IP Phone
- Cisco Voice Portal (CVP)
- xony VIM/CCDM/CCMP

Video, Streaming, TelePresence, and Transcoding Devices

- Cisco AnyRes VOD (CAL)
- Cisco D9036 Modular Encoding Platform
- 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 Headend System Release
- 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 Video Surveillance Media Server
- Cisco Virtual PGW 2200 Softswitch
- Cloud Object Store (COS)

Wireless

- Cisco Aironet 2700 Series Access Point

Cisco Hosted Services

- Cisco Cloud and Managed Service Platform
- Cisco Intelligent Automation for Cloud
- Cisco UCS Invicta Series Autosupport Portal
- Cisco Universal Small Cell CloudBase
- Cisco WebEx Meetings (Meeting Center, Training Center, Event Center, Support Center)

Details

The vulnerability names and the associated Common Vulnerabilities and Exposures (CVE) IDs for the December 3, 2015, OpenSSL Project announcement are as follows:

OpenSSL BN_mod_exp May Produce Incorrect Results on x86_64

A vulnerability in the Montgomery multiplication module of OpenSSL could allow an unauthenticated, remote attacker to cause the library to produce unexpected and possibly weak cryptographic output.

The vulnerability is due to an implementation error in the *BN_mod_exp* function. An unauthenticated, remote attacker

could exploit the vulnerability by sending malicious requests to a targeted application that relies on OpenSSL. A successful exploit could allow the attacker to cause OpenSSL to produce weaker cryptographic protections than expected, possibly allowing the attacker to defeat security protections provided by OpenSSL more easily.

This vulnerability has been assigned CVE ID CVE-2015-3193.

OpenSSL Certificate Processing Denial of Service Vulnerability

A vulnerability in OpenSSL could allow an unauthenticated, remote attacker to cause a DoS condition.

The vulnerability is due to improper handling of certificate signatures. An unauthenticated, remote attacker could exploit the vulnerability by using a malicious certificate during the connection to an application using OpenSSL. Successful exploitation could allow the attacker to cause the targeted application to terminate.

This vulnerability has been assigned CVE ID CVE-2015-3194.

OpenSSL X509_ATTRIBUTE Memory Leak Vulnerability

A vulnerability in OpenSSL could allow an unauthenticated, remote attacker to cause a DoS condition.

The vulnerability is due to improper memory handling. An unauthenticated, remote attacker could exploit the vulnerability by sending malicious requests to an application that uses the OpenSSL library. Successful exploitation could allow the attacker to cause the application to consume available memory resources, resulting in a DoS condition.

This vulnerability has been assigned CVE ID CVE-2015-3195.

OpenSSL Race Condition Handling PSK Identify Hint

A vulnerability in OpenSSL could allow an unauthenticated, remote attacker to cause a DoS condition.

The vulnerability is due to improper memory operations performed when processing preshared keys. An unauthenticated, remote attacker could exploit the vulnerability by sending malicious requests to an application that uses OpenSSL. Successful exploitation could allow the attacker to cause the application to terminate, resulting in a DoS condition.

This vulnerability has been assigned CVE ID CVE-2015-3196.

OpenSSL Anonymous Diffie-Hellman Cipher Suite Denial of Service Vulnerability

A vulnerability in the anonymous Diffie-Hellman cipher suite in OpenSSL could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

The vulnerability is due to improper handling of input by the OpenSSL library. An unauthenticated, remote attacker could exploit the vulnerability by returning malicious values to a client application using OpenSSL. A successful exploit could allow the attacker to cause the application to terminate, resulting in a DoS condition.

This vulnerability has been assigned CVE ID CVE-2015-1794.

Workarounds

Any workarounds will be posted in the Cisco bugs, which are accessible through the Cisco Bug Search Tool.

Fixed Software

Information about fixed software will be in the Cisco bugs, which are accessible through the Cisco Bug Search Tool.

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 upgrade 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 malicious use of the vulnerability that is described in this advisory.

Source

These vulnerabilities were publicly disclosed by the OpenSSL Project on December 3, 2015.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151204-openssl

---

Revision History

Version	Description	Section	Status	Date
1.12	Updated availability dates for WSA. Will be made available in 10.5 release.	Affected Products	Final	2016-September-22
1.11	Updated availability dates for Nexus Products. Will be made available in a 7.3 Maintenance Release.	Affected Products	Final	2016-February-12
1.10	Updated availability dates for Unified Communications products.	Affected Products	Final	2016-February-10
1.9	Removed the duplicate bug entry (CSCux59623) for Cisco Adaptive Security Appliance (ASA).	Affected Products	Final	2016-February-01
1.8	Update first fixed release column.	Affected Products	Final	2016-January-27
1.7	Update first fixed release column.	Affected Products	Interim	2016-January-15
1.6	Updated the Affected Products section.	Affected Products	Interim	2016-January-13
1.5	Updated the Affected Products section.	Affected Products	Interim	2015-December-24
1.4	Updated the Affected Products Section. Cisco DX Series IP Phones moved from Vulnerable to Not Affected.	Affected Products	Interim	2015-December-18
1.3	Updated the Affected Products section.	Affected Products	Interim	2015-December-16
1.2	Updated the Affected Products section and added CVE-2015-1794.	Affected Products	Interim	2015-December-11
1.1	Updated the Affected Products section.	Affected Products	Interim	2015-December-09
1.0	Initial public release.	-	Interim	2015-December-04
