Cisco Security Advisory

Multiple Vulnerabilities in OpenSSL (January 2015) Affecting Cisco Products

Medium

Advisory ID: cisco-sa-20150310-ssl
Last Updated: 2015 November 13 15:34 GMT
Published: 2015 March 10 16:00 GMT
Version1.17: Final
CVSS Score: Base - 5.0
Workarounds: Yes
Cisco Bug IDs: CSCum57065 CSCus42699 CSCus42701 CSCus42702 CSCus42705 CSCus42706 CSCus42709 CSCus42710 CSCus42711 CSCus42712 CSCus42713 CSCus42721 CSCus42723 CSCus42724 CSCus42726 CSCus42727 CSCus42732 CSCus42737 CSCus42738 CSCus42739 CSCus42742 CSCus42748 CSCus42749 CSCus42751 CSCus42752 CSCus42753 CSCus42754 CSCus42755 CSCus42758 CSCus42763 CSCus42766 CSCus42768 CSCus42772 CSCus42775 CSCus42781 CSCus42785 CSCus42786 CSCus42787 CSCus42791 CSCus42792 CSCus42800 CSCus42801 CSCus42804 CSCus42812 CSCus42814 CSCus42816 CSCus42818 CSCus42821 CSCus42827 CSCus42828 CSCus42829 CSCus42831 CSCus42833 CSCus42834 CSCus42836 CSCus42840 CSCus42850 CSCus42851 CSCus42853 CSCus42879 CSCus42883 CSCus42900 CSCus42901 CSCus42904 CSCus42906 CSCus42908 CSCus42917 CSCus42952 CSCus42954 CSCus42958 CSCus42966 CSCus42967 CSCus42968 CSCus42972 CSCus42982 CSCus42983 CSCus42996 CSCus43000 CSCus43003 CSCus43015 CSCus43016 CSCus43020 CSCus43022 CSCus43041 CSCus43052 CSCus44478 CSCus60116 CSCus61884 CSCus77211 CSCut14256 CSCut82321

CVE-2014-3569
CVE-2014-3570
CVE-2014-3571
CVE-2014-3572
CVE-2014-8275
CVE-2015-0204
CVE-2015-0205
CVE-2015-0206
CWE-20
CWE-310
CWE-399
IntelliShield

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

ST 33686
ST 33687
ST 33688
ST 33689
ST 33690
ST 33691
ST 33692
ST 33693
ST 33694
ST 33695
ST 33696
ST 33697
ST 33698
ST 33699
ST 33700
ST 33701
ST 33702
ST 33703
ST 33777
ST 33778
ST 33779
ST 33780
ST 33781
ST 33782
ST 33783
ST 33784
ST 33785
ST 33786
ST 33787
ST 33788
ST 33789
ST 33790
ST 33791
ST 33792
ST 33793
ST 33794
ST 33795
ST 33796
ST 33797
ST 33798
ST 33799
ST 33800
ST 33801
ST 33802
ST 33803
ST 33804
ST 33805
ST 33806

Summary

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 condition or perform a man-in-the-middle attack. On January 8, 2015, the OpenSSL Project released a security advisory detailing eight distinct vulnerabilities. The vulnerabilities are referenced in this document as follows:

- CVE-2014-3571: OpenSSL DTLS Message Processing Denial of Service Vulnerability
- CVE-2015-0206: OpenSSL dtls1_buffer_record Function DTLS Message Processing Denial of Service Vulnerability
- CVE-2014-3569: OpenSSL no-ssl3 Option NULL Pointer Dereference Vulnerability
- CVE-2014-3572: OpenSSL Elliptic Curve Cryptographic Downgrade Vulnerability
- CVE-2015-0204: OpenSSL RSA Temporary Key Cryptographic Downgrade Vulnerability
- CVE-2015-0205: OpenSSL Diffie-Hellman Certificate Validation Authentication Bypass Vulnerability
- CVE-2014-8275: OpenSSL Certificate Fingerprint Validation Vulnerability
- CVE-2014-3570: OpenSSL BN_sql Function Incorrect Mathematical Results Issue

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-20150310-ssl

Affected Products

Vulnerable Products

The following Cisco products have been confirmed to be impacted by one or more of the vulnerabilities contained in the January 8, 2015, OpenSSL Project security advisory:

Product	Defect	Fixed releases availability

Collaboration and Social Media		
Cisco WebEx Meetings Server versions 1.x	CSCus42712	2.5MR2
Cisco WebEx Meetings Server versions 2.x	CSCus42712	2.5MR2
Cisco Webex Social	CSCus42817	No further releases are planned.
Endpoint Clients and Client Software		
Cisco Agent for OpenFlow	CSCus42902	
Cisco AnyConnect Secure Mobility Client for Android	CSCus42726	4.0.01233 (Android)
Cisco AnyConnect Secure Mobility Client for Apple iOS	CSCus42726	3.0.12240 (Apple iOS)
Cisco AnyConnect Secure Mobility Client for desktop platforms	CSCus42726	3.1.07021
Cisco Jabber Software Development Kit	CSCus42945	11.0(0) (26-Aug-2015)
Cisco Jabber Video for TelePresence (Movi)	CSCus42871	4.9 (March 2015)
Cisco Jabber Voice for Android	CSCus42947	10.6(1)
Cisco Jabber for Android	CSCus42952	10.6.1
Cisco Jabber for Mac	CSCus42939	10.6(1) (Available) 11.0 (July 2014)
Cisco Jabber for Windows	CSCut82321	11.0(0) 10.6(1)
Cisco Jabber for iOS	CSCus42953	10.6.2
Cisco WebEx Connect Client for Windows	CSCus42966	No further releases scheduled. Advise migration to Cisco Jabber.
Cisco WebEx Meetings for Android	CSCus42742	7.0 (Android)
Cisco WebEx Meetings for WP8	CSCus42941	1.0.1k (Available)
Network Application, Service, and Acceleration		
Cisco ACE30 Application Control Engine Module	CSCus42709	
Cisco Wide Area Application Services (WAAS)	CSCus42766	5.1.1i (27-May-2015) 6.0.0 (10-Jun-2015)
Network and Content Security Devices		
Cisco ASA CX Context-Aware Security	CSCus42804	9.3.3.1-13 (July 2015)
Cisco Adaptive Security Appliance (ASA) Software	CSCus42901	9.2(3.1) 9.1(5.106) 9.0(4.29) 8.4(7.26)
Cisco Content Security Management Appliance (SMA)	CSCus44454	9.1.2 (15-Jun-2015)
Cisco Email Security Appliance (ESA)	CSCus42818	10.0 (Oct 2015)
Cisco FireSIGHT System Software	CSCus77211	5.4.0.2 5.4.1.1
Cisco IPS	CSCus42768	Cisco IPS 7.1.10 (29-May-2015) Cisco IPS 7.3.4 (TBD)
Cisco Identity Services Engine (ISE)	CSCus42710	1.4 (April 2015) 1.5 (October 2015)
Cisco IronPort Encryption Appliance (IEA)	CSCus44478	
Cisco NAC Appliance (Clean Access Server)	CSCus42836	Patch file is available for vulnerable versions.
Cisco NAC Guest Server	CSCus42834	No further releases are planned.
Cisco NAC Manager (Clean Access Manager)	CSCus42840	Patch file is available for vulnerable versions.
Cisco Physical Access Gateway	CSCus43000	1.5.3 (21-May-2015)
Cisco Secure Access Control Server (ACS)	CSCus42781	5.6 (31-Jul-2015) 5.7 (14-Aug-2015)
Cisco Virtual Security Gateway for Microsoft Hyper-V	CSCus43003	5.2(1)SV3(1.4) (May 2015)
Cisco Virtual Security Gateway for VMware	CSCus43003	5.2(1)SV3(1.4) (May 2015)
Cisco Web Security Appliance (WSA)	CSCus42705	9.0.0 (30-Apr-2015)
Network Management and Provisioning		
Cisco Application Networking Manager	CSCus42821	5.2.6
Cisco Intelligent Automation for Cloud	CSCus42852	4.3 (July 2015)
Cisco MATE Design	CSCus42772	WAE 6.1.1 (31-Mar-2015) MATE 6.0.5 (10-Mar-2015)
Cisco MATE Live	CSCus42772	WAE 6.1.1 (31-Mar-2015) MATE 6.0.5 (10-Mar-2015)
Cisco MATE collector	CSCus42772	WAE 6.1.1 (31-Mar-2015) MATE 6.0.5 (10-Mar-2015)
Cisco Netflow Collection Agent	CSCus42819	1.0.3 (May 2015)
Cisco Packet Tracer	CSCus47080	6.2
Cisco Policy Suite (QPS)	CSCus42789	
Cisco Prime Access Registrar	CSCus42968	7.0.0 (Available) 6.1.3 (Release TBD)
Cisco Prime Collaboration Assurance	CSCus42924	No release planned.
Cisco Prime Collaboration Deployment	CSCus42954	11.0
Cisco Prime Collaboration Provisioning 10.5	CSCus42816	11.0 (29-May-2015)
Cisco Prime Data Center Network Manager (DCNM)	CSCus42763	DCNM 7.1(2) (Late April 2015)
Cisco Prime IP Express	CSCus42967	8.3 (Available)
Cisco Prime Infrastructure	CSCus42748	3.0
Cisco Prime LAN Management Solution	CSCus42883	4.2.5(3) (30-Jun-2015)
Cisco Prime License Manager	CSCus42699	11.0 (mid-April 2015)
Cisco Prime Network Analysis Module (NAM)	CSCus42792	006.002 (1-Jun-2015)
Cisco Prime Network Registrar (CPNR)	CSCus42701	8.3 (Available) 8.2.3 (31-May-2015) 8.1.3.3 (30-Apr-2015) Virtual Appliance 7.3.2.5 (22-Apr-2015)
Cisco Prime Network Services Controller	CSCus42739	3.5.1x (April 2015) Note: PNSC will be no longer be released individually and instead will be part Intercloud Fabric (ICF) 2.2.1x.
Cisco Prime Network	CSCus42882	
Cisco Prime Optical for SPs	CSCus42879	10.3.0.0.193 (Available) 10.0.0.1.2 (Available
Cisco Prime Performance Manager for SPs	CSCus42880	1.6 SP1
Cisco Prime Security Manager	CSCus42841	
Cisco Security Manager	CSCus42723	4.9 (Aug 2015) 4.7 SP1CP1 (Available)
Cisco Show and Share (SnS)	CSCus42800	5.3.x (20-May-2015) 5.5 (20-May-2015) 5.6 (20-May-2015) 5.6.1 (20-Aug-2015)
Local Collector Appliance (LCA)	CSCus42873	2.2.8
Routing and Switching - Enterprise and Service Provider		
Cisco 910 Industrial Router	CSCus45971	1.2.1RB1 (15-May-2015)
Cisco ASR 5000 Series	CSCus42812	20.0.0 (Available)

Show All 48...

Subscribe to Cisco Security Notifications

Subscribe

Cisco Application Policy Infrastructure Controller	CSCus42749	1.0(3f) 1.1(1j)
Cisco Connected Grid Routers (CGR)	CSCus43029	No further releases scheduled (End of Life). Customers are encouraged to upgrade to a supported Cisco IOS Software release.
Cisco IOS Software and Cisco IOS-XE Software	CSCus61884	15.5(03)S
Cisco IOS XR Software	CSCus42773	
Cisco IOS-XE (WebUI feature only)	CSCut32908	
Cisco MDS 9000 Series Multilayer Switches	CSCus42713	7.2 (29-May-2015) 7.3 (3-Jul-2015)
Cisco Mobile Wireless Transport Manager	CSCus42993	6.1.7
Cisco Nexus 1000V Intercloud	CSCus42717	2.2.1 (Available)
Cisco Nexus 1000V Series Switches	CSCut14256	5.2(1)SV3(1.4) (May 2015)
Cisco Nexus 3X00 Series Switches	CSCus43046	
Cisco Nexus 4000 Series Switches	CSCus42972	4.1(2)E1(1o) (15-May-2015)
Cisco Nexus 5000 Series Switches	CSCus42713	7.2 (29-May-2015) 7.3 (3-Jul-2015)
Cisco Nexus 6000 Series Switches	CSCus42713	7.2 (29-May-2015) 7.3 (3-Jul-2015)
Cisco Nexus 7000 Series Switches	CSCus42713	7.2 (29-May-2015) 7.3 (3-Jul-2015)
Cisco Nexus 9000 Series Switches	CSCus42784	7.0(3)I2(1) (Available)
Cisco ONS 15400 Series	CSCus42787	10.51 (20-Nov-2015)
Cisco OnePK All-in-One VM	CSCus42732	Admin to update package via CLI
Routing and Switching - Small Business		
Cisco WAG310G Residential Gateway	CSCus43007	
Unified Computing		
Cisco UCS C-Series (Standalone Rack) Servers	CSCus42715	2.0.4 (Apr 2015)
Cisco UCS Central	CSCus42724	1.3 (March 2015)
Cisco UCS Invicta Series Solid State Systems	CSCus42989	5.0.1.2b (April 2015)
Cisco Unified Computing System B-Series (Blade) Servers	CSCus61833	2.2(4a) (Available) 2.2(5a) (22-May-2015) 3.1(1a) (TBD)
Voice and Unified Communications Devices		
Cisco ATA 187 Analog Telephone Adaptor	CSCus42814	Fix release due March 2016
Cisco ATA 190 Series Analog Telephone Adapter	CSCus42791	1.2.1 (30-Jun-2015)
Cisco Agent Desktop	CSCus42910	10.0(2)
Cisco Computer Telephony Integration Object Server (CTIOS)	CSCut45829	11.0 (30-Apr-2015)
Cisco DX Series IP Phones	CSCut08817	10.2.4 (5-Jun-2015)
Cisco Emergency Responder	CSCus42904	11.0
Cisco Finesse	CSCus42853	
Cisco Hosted Collaboration Mediation Fulfillment	CSCus42794	10.6.1
Cisco IP Interoperability and Collaboration System (IPICS)	CSCus43020	4.9(2) (July 2015)
Cisco IP Phone 8800 Series	CSCuw30989	11.0
Cisco MediaSense	CSCus42906	11.0(1) (Release Date TBD)
Cisco MeetingPlace	CSCus42786	8.6 Maintenance Release (15-Jun-2015)
Cisco Paging Server (Informacast)	CSCus42905	11.0.1 (May 2015)
Cisco Paging Server	CSCus42905	11.0.1 (May 2015)
Cisco SPA112 2-Port Phone Adapter	CSCus42824	1.3.7 (31-Dec-2015)
Cisco SPA122 ATA with Router	CSCus42824	1.3.7 (31-Dec-2015)
Cisco SPA232D Multi-Line DECT ATA	CSCus42824	1.3.7 (31-Dec-2015)
Cisco SocialMiner	CSCus42851	11.0(1) (30-Aug-2015)
Cisco Unified 6900 series IP Phones	CSCus42734	9.4(1)ES12 (11 Nov 2015)
Cisco Unified 7800 series IP Phones	CSCus42707	10.4.1 (August 2015)
Cisco Unified 8945 IP Phone	CSCus42735	9.4(2)2SR2 (11-Dec-2015)
Cisco Unified 8961 IP Phone	CSCus42706	9.4(2)SR2 (Release Date TBD)
Cisco Unified 9951 IP Phone	CSCus42706	9.4(2)SR2 (Release Date TBD)
Cisco Unified 9971 IP Phone	CSCus42706	9.4(2)SR2 (Release Date TBD)
Cisco Unified Attendant Console (all editions)	CSCus42803	11.0.1 (Sep 2015)
Cisco Unified Attendant Console Standard	CSCus42959	Patch files are available for vulnerable releases.
Cisco Unified Communication Manager IM and Presence Service (CUPS)	CSCus42751	11.0 (Available)
Cisco Unified Communications Domain Manager	CSCus42711	10.1(2)
Cisco Unified Communications Manager (UCM)	CSCus60116	10.5.2 (Available) 10.5.2 SU2 (Available) 9.1.2 SU3 (TBD) 8.6.2 (TBD)
Cisco Unified Communications Manager Session Management Edition (SME)	CSCus60116	10.5.2 (Available) 10.5.2 SU2 (Available) 9.1.2 SU3 (TBD) 8.6.2 (TBD)
Cisco Unified Contact Center Enterprise	CSCut45829	11.0 (30-Apr-2015)
Cisco Unified Contact Center Express	CSCus42785	11.0(1) (June 2015)
Cisco Unified IP Conference Phone 8831	CSCus42757	
Cisco Unified IP Conference Station 7937G	CSCus42758	10.3.2 (Sep 2015)
Cisco Unified IP Phone 7900 Series	CSCus42733	9.4(2)SR2 (11-Nov-2015)
Cisco Unified Intelligence Center	CSCus42908	
Cisco Unified Intelligent Contact Management Enterprise	CSCut45829	11.0 (30-Apr-2015)
Cisco Unified Sip Proxy	CSCus42917	
Cisco Unified Workforce Optimization	CSCus42996	10.5 SR6 11.0
Cisco Unity Connection (UC)	CSCus42900	11.0(0.72)
Cisco Virtualization Experience Media Engine	CSCus42958	Windows 10.6.0.10706 (Available) Windows 10.6.0.10730 (Available) Linux 10.6.0-203 (Available) Linux 10.6.0-221 (Available)
Video, Streaming, TelePresence, and Transcoding Devices		
Cisco AnyRes Live (CAL)	CSCus42909	9.5.0
Cisco D9036 Modular Encoding Platform	CSCus42887	V02.03.30
Cisco Edge 300 Digital Media Player	CSCus42801	1.6RB2 (Available)
Cisco Edge 340 Digital Media Player	CSCus43052	Patch file available for vulnerable releases. (4-Apr-2015)
Cisco Enterprise Content Delivery System (ECDS)	CSCum57065	2.6.4 (mid-May 2015)
Cisco Expressway Series	CSCus42702	X8.5.1
Cisco Internet Streamer CDS	CSCus42921	VDS-IS 3.3.1 (30-Jun-2015) VDS-IS 4.2.0 (31-Jul-2015)
Cisco Model D9485 DAVIC QPSK	CSCus43043	1.2.19
		1.10.11 (30-Apr-2015)

Cisco TelePresence 1310	CSCus42737	6.1.8 (30-Apr-2015)
Cisco TelePresence Advanced Media Gateway Series	CSCus42833	1.1(1.40) (Available)
Cisco TelePresence Conductor	CSCus42987	XC3.0.1
Cisco TelePresence Content Server (TCS)	CSCus42976	6.2
Cisco TelePresence EX Series	CSCus42827	7.3.1
Cisco TelePresence ISDN GW 3241	CSCus42753	2.2 Maintenance Release (mid May 2015)
Cisco TelePresence ISDN GW MSE 8321	CSCus42753	2.2 Maintenance Release (mid May 2015)
Cisco TelePresence ISDN Link	CSCus42828	1.1.5 (June 2015)
Cisco TelePresence MCU (8510, 8420, 4200, 4500 and 5300)	CSCus42831	4.5 Maintenance Release (July 2015)
Cisco TelePresence MX Series	CSCus42827	7.3.1
Cisco TelePresence Profile Series	CSCus42827	7.3.1
Cisco TelePresence SX Series	CSCus42827	7.3.1
Cisco TelePresence Serial Gateway Series	CSCus42754	1.0(1.42)
Cisco TelePresence Server 8710, 7010	CSCus42752	4.1 (Mar 2015)
Cisco TelePresence Server on Multiparty Media 310, 320	CSCus42752	4.1 (Mar 2015)
Cisco TelePresence Server on Virtual Machine	CSCus42752	4.1 (Mar 2015)
Cisco TelePresence Supervisor MSE 8050	CSCus42755	2.3(1.38)
Cisco TelePresence System 1000	CSCus42737	1.10.11 (30-Apr-2015) 6.1.8 (30-Apr-2015)
Cisco TelePresence System 1100	CSCus42737	1.10.11 (30-Apr-2015) 6.1.8 (30-Apr-2015)
Cisco TelePresence System 1300	CSCus42737	1.10.11 (30-Apr-2015) 6.1.8 (30-Apr-2015)
Cisco TelePresence System 3000 Series	CSCus42737	1.10.11 (30-Apr-2015) 6.1.8 (30-Apr-2015)
Cisco TelePresence System 500-32	CSCus42737	1.10.11 (30-Apr-2015) 6.1.8 (30-Apr-2015)
Cisco TelePresence System 500-37	CSCus42737	1.10.11 (30-Apr-2015) 6.1.8 (30-Apr-2015)
Cisco TelePresence TE Software (for E20 - EoL)	CSCus42829	4.1.6
Cisco TelePresence TX 9000 Series	CSCus42737	1.10.11 (30-Apr-2015) 6.1.8 (30-Apr-2015)
Cisco TelePresence Video Communication Server (VCS)	CSCus42702	X8.5.1
Cisco Telepresence Integrator C Series	CSCus42827	7.3.1
Cisco VDS Service Broker	CSCus43022	
Cisco Video Surveillance 3000 Series IP Cameras	CSCus42721	2.7 (30-Jul-2015)
Cisco Video Surveillance 4000 Series High-Definition IP Cameras	CSCus42983	2.4.6 (30-Jul-2015)
Cisco Video Surveillance 4300E/4500E High-Definition IP Cameras	CSCus42982	3.2.7 (30-Jul-2015)
Cisco Video Surveillance 6000 Series IP Cameras	CSCus42721	2.7 (30-Jul-2015)
Cisco Video Surveillance 7000 Series IP Cameras	CSCus42721	2.7 (30-Jul-2015)
Cisco Video Surveillance Media Server	CSCus43015	7.7
Cisco Video Surveillance Operations Manager	CSCus43016	7.7.0 (15-Aug-2015)
Cisco Video Surveillance PTZ IP Cameras	CSCus42721	2.7 (30-Jul-2015)
Cisco Videoscape Control Suite	CSCus43009	3.6 (Available)
Cloud Object Store (COS)	CSCus43014	2.1.2 (Available) 3.0.0 (27-May-2015)
Media Services Interface	CSCus43013	No further releases planned.
Tandberg Codian ISDN GW 3210/3220/3240	CSCus42753	2.2 Maintenance Release (mid May 2015)
Tandberg Codian MSE 8320 model	CSCus42753	2.2 Maintenance Release (mid May 2015)
Wireless		
Cisco IOS Access Points	CSCus42764	15.5(03)S (Available)
Cisco Mobility Services Engine (MSE)	CSCus42729	8.0.110.002
Cisco Wireless Lan Controller (WLC)	CSCus42727	7.0.252.0 (Available) 7.4.140.0 (Available) 8.1.102.0 (Available) 8.0.120.0 (June 2015) 7.6.130.26 (Contact Cisco TAC for this version)
Cisco Hosted Services		
Cisco Common Services Platform Collector	CSCus95785	
Cisco Network Configuration and Change Management Service	CSCus42860	1.5 (Available)
Cisco Proactive Network Operations Center	CSCus42796	
Cisco Universal Small Cell 5000 Series running V3.4.2.x software	CSCus42775	3.5.11.11 3.4.5.7
Cisco Universal Small Cell 7000 Series running V3.4.2.x software	CSCus42775	3.5.11.11 3.4.5.7
Network Performance Analytics (NPA)	CSCus42893	1.11.3 (30-Aug-2015)

Products Confirmed Not Vulnerable

The following Cisco products have been analyzed and are not affected by any of the listed vulnerabilities:

Collaboration and Social Media

- Cisco WebEx Node for MCS

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 Unified Video Advantage
- Cisco WebEx Meetings (client)
- Cisco WebEx Meetings for BlackBerry
- Cisco WebEx Productivity Tools
- Cisco Webex App for iOS

Network Application, Service, and Acceleration

- Cisco Application and Content Networking System (ACNS)
- Cisco Extensible Network Controller (XNC)

Network and Content Security Devices

- 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 Discovery Service
- Cisco Insight Reporter
- Cisco Linear Stream Manager
- Cisco Multicast Manager
- Cisco Prime Analytics
- Cisco Prime Cable Provisioning
- Cisco Prime Central for SPs
- Cisco Prime Home
- Cisco SON Suite
- Cisco Unified Provisioning Manager (CUPM)
- CiscoWorks Network Compliance Manager
- Digital Media Manager 5.4

Routing and Switching - Enterprise and Service Provider

- Cisco Broadband Access Center Telco Wireless
- Cisco Prime Provisioning for SPs
- Cisco Service Control Operating System

Routing and Switching - Small Business

- Cisco VEN401 Wireless Access Point
- Cisco VEN501 Wireless Access Point

Voice and Unified Communications Devices

- Cisco Desktop Collaboration Experience DX650
- 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 Unified Communications Domain Manager
- Cisco Unified 3900 series IP Phones
- Cisco Unified Client Services Framework
- Cisco Unified Communications Sizing Tool
- Cisco Unified Communications Widgets Click To Call
- Cisco Unified E-Mail Interaction Manager
- Cisco Unified Integration for IBM Sametime
- Cisco Unified Web Interaction Manager
- Cisco Virtual PGW 2200 Softswitch
- Cisco Voice Portal (CVP)
- xony VIM/CCDM/CCMP

Video, Streaming, TelePresence, and Transcoding Devices

- Cisco AnyRes VOD (CAV)
- 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 Digital Media Players
- 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

Wireless

- Cisco Wireless Location Appliance

Cisco Hosted Services

- Cisco Connected Analytics For Collaboration
- Cisco Install Base Management (IBM)
- Cisco Registered Envelope Service (CRES)
- Cisco Services Platform Collector (CSPC)
- Cisco SmartConnection
- Cisco SmartReports
- Cisco WebEx WebOffice Workspace
- Cisco Webex Messenger Service
- Connected Analytics for Network Deployment (CAND)
- Services Analytic Platform
- Webex Meeting Center

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

Details

The OpenSSL Project disclosed eight vulnerabilities on January 8, 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.

OpenSSL DTLS Message Processing 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 network messages. An attacker could exploit this vulnerability by sending malicious network messages to a targeted system.

This vulnerability has been assigned CVE ID CVE-2014-3571.

OpenSSL dtls1_buffer_record Function DTLS Message Processing Denial of Service Vulnerability

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

The vulnerability is due to an error condition that occurs when the affected software processes crafted Datagram Transport Layer Security (DTLS) packets. An unauthenticated, remote attacker could exploit this vulnerability by sending crafted DTLS packets to an affected OpenSSL-based server. An exploit could allow the attacker to consume excessive memory resources, resulting in a DoS condition.

This vulnerability has been assigned CVE ID CVE-2015-0206.

OpenSSL no-ssl3 Option NULL Pointer Dereference 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 implementation of the OpenSSL build configuration. An unauthenticated, remote attacker could exploit this vulnerability by sending a crafted SSL 3.0 handshake request to the targeted client. Processing the request could cause the affected software to terminate abnormally, leading to a DoS condition.

This vulnerability has been assigned CVE ID CVE-2014-3569.

OpenSSL Elliptic Curve Cryptographic Downgrade Vulnerability

A vulnerability in OpenSSL could allow an unauthenticated, remote attacker to conduct downgrade attacks.

The vulnerability is due to insecure implementation of ephemeral Elliptic Curve Diffie-Hellman (ECDH) ciphersuites by the affected software. An unauthenticated, remote attacker could exploit this vulnerability by transmitting crafted handshake requests to the targeted client system. When processed, the requests could allow the attacker to downgrade the server to use the weaker encryption protocol, which could allow the attacker to obtain sensitive information from the system.

This vulnerability has been assigned CVE ID CVE-2014-3572.

OpenSSL RSA Temporary Key Cryptographic Downgrade Vulnerability

A vulnerability in OpenSSL could allow an unauthenticated, remote attacker to bypass security restrictions.

The vulnerability is due to improper handling of an RSA temporary key. An attacker with a privileged network position could exploit the vulnerability by returning a weak temporary RSA key to a system using an application that uses the vulnerable OpenSSL library. When processed, the insecure temporary key could result in reduced cryptographic protections, which could allow the attacker to bypass security protections.

This vulnerability has been assigned CVE ID CVE-2015-0204.

OpenSSL Diffie-Hellman Certificate Validation Authentication Bypass Vulnerability

OpenSSL contains a vulnerability that could allow an unauthenticated, remote attacker to bypass certain security restrictions and access sensitive information on a targeted system.

The vulnerability is due to improper certificate verification by the affected software. An unauthenticated, remote attacker could exploit this vulnerability by transmitting a crafted Diffie-Hellman certificate without the certificate verify message to the affected server. The processing of such certificates could allow the attacker to bypass certain security restrictions and access sensitive information on the system.

This vulnerability has been assigned CVE ID CVE-2015-0205.

OpenSSL Certificate Fingerprint Validation Vulnerability

A vulnerability in OpenSSL could allow an unauthenticated, remote attacker to bypass fingerprint-based certificate validation mechanisms implemented by the affected software.

The vulnerability exists due to insufficient constraints applied on certificate data by the affected software. An attacker could exploit this vulnerability by including crafted data within a certificate's unsigned portion and submitting it to be processed by the affected software. If successful, an attacker could bypass the fingerprint-based certificate-blacklist protection mechanism implemented by the affected software.

This vulnerability has been assigned CVE ID CVE-2014-8275.

OpenSSL BN_sql Function Incorrect Mathematical Results Issue

An issue in OpenSSL could result in the calculation of incorrect mathematical results.

The issue is in the *BN_sql* function because the function does not properly calculate the square of a BIGNUM value. An unauthenticated, remote attacker could exploit this issue using an unspecified vector. Successful exploitation could cause the software to calculate incorrect results.

Reports suggest that no exploits are known and straightforward bug attacks fail because the attacker cannot control when the bug triggers and no private key material is involved.

This vulnerability has been assigned CVE ID CVE-2014-3570.

Workarounds

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

Fixed Software

When considering software upgrades, customers are advised to consult the Cisco Security Advisories, Responses, and Notices 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

In early March 2015, CVE-2015-0204: OpenSSL RSA Temporary Key Cryptographic Downgrade Vulnerability, received media attention for research done into the factoring attack on RSA-EXPORT Keys (dubbed FREAK).

These vulnerabilities were publicly disclosed by the OpenSSL Project on January 5, 2015. Consistent with our security vulnerability disclosure policy, the Cisco PSIRT began disclosing the effect to Cisco products through public release notes, before increased public discussion of FREAK led to this security advisory.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150310-ssl

---

Revision History

Version	Description	Section	Status	Date
1.17	Updated first fixed releases for the APIC from 1.1(0.625), 1.0(2.136a) to 1.1(1j) and 1.0(3f)	Affected Products	Final	2015-November-13
1.16	Added Cisco IP Phone 8800 Series to affected products section.			2015-September-22
1.15	Updated fixed releases availability.			2015-June-02
1.14	Moved the Cisco Mobility Services Engine (MSE) to an affected product. Updated Fixed releases availability.			2015-May-28
1.13	Updated Vulnerable Products Fixed releases availability column.			2015-May-14
1.12	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.			2015-May-06
1.11	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.			2015-April-30
1.10	Updated the Vulnerable Products fixed column. Added Cisco IOS Access Points to under investigation.			2015-April-27
1.9	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.			2015-April-17
1.8	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.			2015-April-13
1.7	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections. Removed End of Life product - Cisco Small Business ISA500 Series Integrated Security Appliances.			2015-April-09
1.6	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.			2015-April-02
1.5	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections. Several End of Life products were removed from the advisory.			2015-March-26
1.4	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections. Added Cisco TelePresence IP Gateway Series to the advisory.			2015-March-19
1.3	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.			2015-March-16
1.2	Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.			2015-March-13
1.1	Moved Cisco Content Security Management Appliance (SMA) from Not Vulnerable to under Investigation. Updated the Affected Products, Vulnerable Products, and Products Confirmed Not Vulnerable sections.			2015-March-11
1.0	Initial public release.			2015-March-10

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 standalone 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.