

OpenSSL 代替は認証偽作脆弱性を連鎖します (July 2015) シスコ製品に影響を及ぼす

Medium アドバイザリーID : cisco-sa-[CVE-20150710-openssl](#) [CVE-2015-1793](#)

m 初公開日 : 2015-07-10 16:00

最終更新日 : 2015-09-16 16:54

バージョン 1.23 : Final

回避策 : [Yes](#)

Cisco バグ ID : [CSCuu82763](#) ,
[CSCuv26109](#) , [CSCuv26209](#) ,
[CSCuv26316](#) , [CSCuv26844](#) ,
[CSCuv26185](#) , [CSCuv33644](#) ,
[CSCuv26164](#) , [CSCuv26150](#) ,
[CSCuv26172](#) , [CSCuv26183](#) ,
[CSCuv26293](#) , [CSCuv26283](#) ,
[CSCuv26259](#) , [CSCuv26303](#) ,
[CSCuv26213](#) , [CSCuv26279](#) ,
[CSCuv26167](#) , [CSCuv26168](#) ,
[CSCuv46148](#) , [CSCuv26099](#) ,
[CSCuv26243](#)

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

2015 年 7 月 9 日で、OpenSSL プロジェクトは証明書を確認するクライアント認証を使用して SSL/Transport 層 セキュリティ (TLS) /Datagram Transport Layer Security (DTLS) クライアントおよび SSL/TLS/DTLS サーバを含むアプリケーションに影響を与える脆弱性を詳述する Security Advisory をリリースしました。

複数のシスコ製品は信頼できない証明書のある特定のチェックをバイパスします非認証を可能にする可能性があるこの脆弱性から影響を受ける OpenSSL パッケージのバージョンをリモート攻撃者織込んでいて man-in-the-middle 攻撃を行なうのに使用する可能性がある「信頼された」証明書を造るために攻撃者を有効にします。

このアドバイザリーは追加情報が入手可能になった時点で更新されます。

この脆弱性を軽減する回避策は利用可能かもしれません。

このアドバイザリは、次のリンクより確認できます。

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

該当製品

修正済みソフトウェア

以下のシスコ製品は OpenSSL プロジェクト Security Advisory に 2015 年 7 月 10 日含まれている脆弱性の何れか一つ以上によって影響を与えられるために確認されました:

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	該当するリリースのために利用可能なパッチファイル。
Cisco Jabber Software Development Kit	CSCuv26303	11.0(0) (26-Aug-2015)
Network and Content Security Devices		
Cisco ASA CX および Cisco Prime Security Manager	CSCuv26213	9.3.3.4 (MR6) (2015) 9 月
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 (2015) 10 月 6.1.3 (2015) 10 月
Cisco Prime Collaboration Deployment	CSCuv26283	11.5.1 (2016) 3 月
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 (2015) 10 月 10.5.2 (2015) DEC
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)
		XE3.13
		14
Cisco IOS XE (WebUI 機能だけ)	CSCuu82763	15 16 (利用可能) XE3.11 13 (次のリリース)
Cisco Nexus 9000 (ACI/Fabric Switch)	CSCuv26128	11.1.2 (2015) 8 月
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 (2016) 2 月
Cisco IM and Presence Service (CUPS)	CSCuv26296	
		11.5 (20-Oct-2015)
Cisco MediaSense	CSCuv26316	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 Player	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	該当するリリース (20-Jul-2015) のために利用可能なパッチファイル
Cisco Hosted Services		
Cisco Registered Envelope Service (CRES)	CSCuv26099	4.4.1 (1-Aug-2015)
Cisco Universal Small Cell 5000 シリーズ (V3.4.2.x ソフトウェアを実行)	CSCuv26256	BV3.4.4.8
Cisco Universal Small Cell 7000 シリーズ (V3.4.2.x ソフトウェアを実行)	CSCuv26256	BV3.4.4.8
Cisco WebEx Messenger	CSCuv26116	7.9.9 EP1 (利用可能な)

Service	
Network Performance Analytics (NPA)	CSCuv26268 1.11.3 (30-Sept-2015)
Partner Supporting Service (PSS) 1.x	CSCuv26208
サービス分析プラットフォーム	CSCuv26091 該当するリリースのために利用可能なパッチファイル。

脆弱性を含んでいないことが確認された製品

Cisco は以下の製品が OpenSSL プロジェクトによって発表される脆弱性に脆弱 2015 年 7 月 9 日ではないことを確認しました:

Collaboration and Social Media

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

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
- ブラックベリーののための Cisco WebEx Meetings
- Cisco WebEx Productivity Tools
- WebEx Meetings Server - SSL Gateway
- WebEx Recording Playback Client

- 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 SireSIGHT システム ソフトウェア
- 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 Clouplia 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 債権取立業者
- 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 シリーズ
- Cisco Application Policy Infrastructure Controller (APIC)
- Cisco Broadband Access Center Telco Wireless
- Cisco Connected Grid Router - CGOS
- Cisco IOSソフトウェアおよび Cisco IOS XE ソフトウェア
- Cisco IOS XE (SSLVPN 機能)
- Cisco IOS XR
- Cisco MDS 9000 Series Multilayer Switches
- Cisco Mobile Wireless Transport Manager
- Cisco Nexus 1000V InterCloud
- Cisco Nexus 1000V シリーズ スイッチ
- Cisco Nexus 2000 シリーズ FEX
- Cisco Nexus 3X00 シリーズ スイッチ

- Cisco Nexus 4000 Series Blade Switches
- Cisco Nexus 5000 Series Switches
- Cisco Nexus 6000 Series Switches
- Cisco Nexus 7000 Series Switches
- Cisco Nexus 9000 シリーズ (スタンドアロン、NxOS を実行します)
- Cisco ONS 15454 Series Multiservice Provisioning Platforms
- Cisco OnePK All-in-One VM
- Cisco Service Control オペレーティング システム

Routing and Switching - Small Business

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

Unified Computing

- Cisco Common Services Platform Collector
- Cisco スタンドアロン ラック サーバ 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 シリーズ IP フォン
- 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 ポート IP テレフォニー ゲートウェイ
- Cisco SPA8800 IP テレフォニー ゲートウェイ (4 FXS ポートと 4 FXO ポートを内蔵)
- Cisco TAPI Service Provider (TSP)
- Cisco USC8088
- Cisco Unified 3900 シリーズ IP フォン
- Cisco Unified 6901 の IP フォン
- Cisco Unified 6911 の IP フォン
- Cisco Unified 6921 の IP フォン
- Cisco Unified 6945 の IP フォン
- Cisco Unified 7800 Series IP Phones
- Cisco Unified 8831 シリーズ IP 会議電話
- Cisco Unified 8945 IP フォン
- Cisco Unified 8961 IP フォン
- 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 ソフトスイッチ
- 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 ヘッドエンド システムリリース
- Cisco インターネット吹流し (CD)
- 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 シリーズ
- 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 オブジェクト ストア (COS)
- Tandberg Codian ISDN GW 3210/3220/3240
- Tandberg Codian MSE 8320 model

Wireless

- Cisco モビリティ サービス エンジン (MSE)
- Cisco Wireless Control System (WCS)
- Cisco Wireless LAN Controller (WLC)

Cisco Hosted Services

- Cisco Cloud Web Security
- Cisco Intelligent Automation for Cloud
- Cisco 予防的 な Network Operations Center
- Cisco SmartConnection
- Cisco SmartReports
- Cisco Unified Services Delivery Platform (CUSDP)
- Cisco WebEx Meetings (Meeting Center, Training Center, Event Center, Support Center)

- 通信/コラボレーション サイズ変更ツールは、美德マシン 配置 ツール、Cisco Unified Communications 準備の評価をアップグレードします
- Connected Analytics for Network Deployment (CAND)
- ライフサイクル 管理 エージェント マネージャ (LCM)
- Serial Number Assessment Service (SNAS)

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

改訂履歴

Revision 1.23	2015-September-16	Updated Affected Products section - Vulnerable/Not Vulnerable Products. 以下の3つの製品は脆弱から脆弱に移りました: Cisco Nexus 6000 シリーズ スイッチ、Cisco Nexus 5000 シリーズ スイッチ、Cisco Nexus 2000 シリーズ FEX。
Revision 1.22	2015-September-14	Updated Affected Products section - Vulnerable/Not Vulnerable Products. 脆弱から脆弱に移られる以下の3つの製品: Cisco Jabber for Android、WebEx 記録再生クライアントおよびホストされる Cisco WebEx Meetings クライアント。
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	2015-	Updated Affected Products section -

Revision 1.13	July-29	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.
リビジョン 1.4	2015-July-16	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
リビジョン 1.3	2015-July-15	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
リビジョン 1.2	2015-July-14	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
リビジョン 1.1	2015-July-13	Updated Affected Products section - Vulnerable/Not Vulnerable Products.
リビジョン 1.0	2015-July-10	Initial public release.

利用規約

本アドバイザーは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。本アドバイザーの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。