

シスコ製品に影響を及ぼす OpenSSL の多重脆弱点: January および February 2017 年

Medium	アドバイザーID : cisco-sa-20170130-openssl	CVE-2017-3730
	初公開日 : 2017-01-30 21:28	
	最終更新日 : 2017-07-05 11:43	CVE-2017-3732
	バージョン 2.9 : Final	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvc94616	CVE-2017-3731
	CSCvc94581 CSCvc94585	
	CSCvc94662 CSCvc94665	
	CSCvc94589 CSCvc94741	CVE-2017-3733
	CSCvc94669 CSCvc94623	
	CSCvc94745 CSCvc94729	
	CSCvc94649 CSCvc94609	
	CSCvc98372 CSCvc94691	
	CSCvc94650 CSCvc94651	
	CSCvc94692 CSCvc94730	
	CSCvc94735 CSCvc94759	
	CSCvc94716 CSCvc98361	
	CSCvc98364 CSCvc94760	
	CSCvc98369 CSCvc96106	
	CSCvc94765 CSCvc94641	
	CSCvc94762 CSCvc94768	
	CSCvc94604 CSCvc94648	
	CSCvc94601 CSCvc94602	
	CSCvc94767 CSCvc96109	
	CSCvc94629 CSCvc94749	
	CSCvc96092 CSCvc96093	
	CSCvc94591 CSCvc96099	
	CSCvc96176 CSCvc94590	
	CSCvc94595 CSCvc94632	
	CSCvc94556 CSCvc94633	
	CSCvc94598 CSCvc94752	
	CSCvc94636 CSCvc94637	
	CSCvc94758 CSCvc94634	

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

2017年1月26日で、OpenSSL ソフトウェア基礎は 3 新しい脆弱性を含んだ Security Advisory をリリースしました。基礎はまた 2016 年 11 月の OpenSSL アドバイザリで既に表われ、[シスコ製品に影響を及ぼす OpenSSL の Cisco Security Advisory 多重脆弱点](#)に含まれていた 1 脆弱性をリリースしました [:11月 2016 年](#)。OpenSSL は「適度な重大度として分類しますすべての新しい脆弱性を」。

最初の脆弱性は 32ビット システム・アーキテクチャで使用される OpenSSL だけ影響を与え、OpenSSL をクラッシュするために引き起こすかもしれません。2つめの脆弱性は OpenSSL がクライアント側で使用されるときだけバージョン 1.1.0 だけ影響を与え、発生します。悪意のあるサーバに接続するとき 2つめの脆弱性により OpenSSL はクラッシュしますかもしれません。第 3 脆弱性は x86_64 アーキテクチャに基づいてシステムだけ影響を及ぼします。第 3 脆弱性の正常なエクスプロイトは攻撃者が敏感な秘密キーの情報にアクセスすることを可能にする可能性があります。

複数のシスコ製品はこれらの脆弱性の何れか一つ以上から影響を受ける OpenSSL パッケージのバージョンを織込んでいます。

CVE ID CVE-2017-3730 によって識別される脆弱性から影響を受けるシスコ製品がありません。

2017年2月16日で、OpenSSL ソフトウェア基礎は CVE ID CVE-2017-3733 によって識別された 1 高い重大度脆弱性を含んだ別の Security Advisory をリリースしました。

この脆弱性から影響を受けるシスコ製品がありません。

このアドバイザリは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170130-openssl>

該当製品

シスコでは、本脆弱性の影響を受ける製品と影響の範囲を特定するために、製品ラインを調査しました。製品が影響を受けているかについて情報に関してはこのアドバイザリの「脆弱性が存在する製品」および「脆弱性が存在しない製品」セクションを参照して下さい。

「脆弱性が存在する製品」セクションは各々の影響を受けた製品のための Cisco バグ ID が含まれています。Cisco Bug は [Cisco Bug Search Tool](#) で検索可能であり、回避策（使用可能な場合）と修正されたソフトウェア リリースなど、プラットフォーム固有の追加情報が記載されます。

CVE ID CVE-2017-3730 および CVE-2017-3733 によって識別される脆弱性から影響を受けるシスコ製品がありません。

脆弱性のある製品

Product	Cisco Bug ID	Fixed Release Availability
Collaboration and Social Media		
Cisco SocialMiner	CSCvc98364	
Cisco WebEx Meetings サーバ リリース 1.x	CSCvc94595	CWMS 2.8 (31-March-2017)
Cisco WebEx Meetings サーバ リリース 2.x	CSCvc94595	CWMS 2.8 (31-March-2017)
Endpoint Clients and Client Software		
Cisco Jabber Guest	CSCvc94762	11.0(1) (31-May-2017)
Cisco Jabber Software Development Kit	CSCvc94759	11.9 (30-June-2017)
Cisco Jabber for Mac	CSCvc94758	11.9 (30-June-2017)
Cisco Jabber for Windows	CSCvc94760	11.9.0 (28-Jun-2017)
Cisco WebEx ビジネススイート	CSCvc94597	NBR 3.6.0 (30-March-2017)
Cisco WebEx Meetings Client - Hosted	CSCvc96091	31.12 (28-Feb-2017)
Cisco WebEx Meetings クライ アント-オン前提	CSCvc96090	31.12 (28-Feb-2017)
Cisco WebEx Meetings サーバ- マルチメディアプラットフォーム (MMP)	CSCvc96092	6.0.325 (利用可能)
Network and Content Security Devices		
Cisco コンテンツ セキュリテ ィ アプライアンス モデル アッ プデート サーバ	CSCvc94591	2.0.3-111 (3-Mar-2017)
Cisco Content Security Management Appliance (SMA)	CSCvc94590	11.5 (9月- 2017)
Cisco Email Security Appliance (ESA)	CSCvc94585	11.5 (9月- 2017)
Cisco FireSIGHT システム ソ フトウェア	CSCvc94589	6.2.0.1 (April-2017) 6.1.0.3 (July-2017) 6.0.1.3 (June-2017) 5.4.0.11/5.4.1.10 (July- 2017)
Cisco Identity Services Engine (ISE)	CSCvc94692	
Cisco Web Security Appliance (WSA)	CSCvc94592	11.5 (9月- 2017)
Network Management and Provisioning		
Cisco Application Policy Infrastructure Controller (APIC)	CSCvc96095	2.3 (June-2017)
Cisco MATE Collector	CSCvc94716	
Cisco MATE Design	CSCvc94716	
Cisco MATE Live	CSCvc94716	
Cisco NetFlow Generation Appliance	CSCvc94643	1.1.1 (13-April-2017) 1.1.1a (13-April-2017)
Cisco Network Analysis Module	CSCvc94637	6.2.1 (13-April-2017) 6.2.2 (13-April-2017)
Cisco Prime Access Registrar	CSCvc94632	8.0 (30-July-2017)
Cisco Prime Collaboration	CSCvc96099	PCA 11.6 で利用可能 な修正既に

Assurance		
Cisco Prime Collaboration Deployment	CSCvc96106	
Cisco Prime Data Center Network Manager	CSCvc94601	10.2.1 (21-April-17)
Cisco Prime IP Express	CSCvc94634	8.3.5 (28-Feb-2017)
Cisco Prime Infrastructure	CSCvc94641	3.2: (31-March-2017) 3.1.6 (31-March-2017)
Cisco Prime License Manager	CSCvc94662	11.5 (1.12001-2) (7-April-2017)
Cisco Prime Network Registrar	CSCvc94629	8.3.5 (28-Feb-2017)
サービスプロバイダーのための Cisco Prime Optical	CSCvc94633	10.6.1.0 (Feb-2017)
Cisco Prime Performance Manager	CSCvc94623	SP1703 (31-March-2017)
Cisco Smart Net Total Care - ローカルコレクタアプライアンス	CSCvc94723	2.2.14 (10-Feb-2017)
Cisco Unified Intelligence Center	CSCvc98361	
Routing and Switching - Enterprise and Service Provider		
Cisco ASR 5000 シリーズ	CSCvc94556	21.2.0 (30-April-2017)
Cisco Application Policy Infrastructure Controller (APIC)	CSCvc94602	2.3 (July - 2017)
Cisco Connected Grid ルータ	CSCvc94730	15.6(3)M2 (31-Mar-2017)
Cisco IOS XR ソフトウェア	CSCvc94649	6.3.1
Cisco IOS および Cisco IOS XE ソフトウェア	CSCvc94729	16.6 (15-Feb-2017)
Cisco MDS 9000 Series Multilayer Switches	CSCvc94605	6.2.21 利用可能な修正無しまだ 8.2.1 (2017) 3月9日 7.0.3.I6 (2017) MDS 9000: 6.2.21 利用可能な修正無しまだ N5K
Cisco MDS 9000 Series Multilayer Switches	CSCvc94606	N6K: 修正予定なし N7K: 8.2.1 (2017) 9月 N3K N9K 7.0.3.I6 (4月 2017)
Cisco Nexus 1000V InterCloud	CSCvc94604	修正予定なし
Cisco Nexus 3000 Series Switches	CSCvc94609	6.0(2)A8(4) (15-Apr-2017)
Cisco Nexus 4000 Series Blade Switches	CSCvc94709	4.1(2)E1(1s) (15-July-2017) MDS 9000: 6.2.21 利用可能な修正無しまだ N5K
Cisco Nexus 5000 Series Switches	CSCvc94606	N6K: 修正予定なし N7K: 8.2.1 (2017) 9月 N3K N9K 7.0.3.I6 (4月 2017)
Cisco Nexus 5000 Series Switches	CSCvc94610	7.3 (02-May-2017) MDS 9000: 6.2.21 利用可能な修正無しまだ N5K
Cisco Nexus 6000 Series Switches	CSCvc94606	N6K: 修正予定なし N7K: 8.2.1 (2017) 9月

		N3K
		N9K 7.0.3.16 (4月 2017)
		MDS 9000: 6.2.21 利用可能な修正無しまだ
		N5K
Cisco Nexus 7000 Series Switches	CSCvc94606	N6K: 修正予定なし N7K: 8.2.1 (2017) 9月 N3K N9K 7.0.3.16 (4月 2017)
Cisco Nexus 9000 シリーズ ファブリック スイッチ (ACI モード)	CSCvc94603	12.3x ドラァヴァ川 (Jun-2017)
Unified Computing		
Cisco Common Services Platform Collector	CSCvc94568	CASP 1.12 (10-March-2017)
Cisco UCS 6200 シリーズおよび 6300 シリーズ ファブリックは相互接続します	CSCvc94686	3.2.3 (14-Apr-2017)
Cisco UCS B シリーズ ブレード サーバ	CSCvc94616	3.2 (June-2017)
Cisco UCS Director	CSCvc96093	6.1 GlacierBay (31-May-2017)
Cisco UCS Manager	CSCvc96103	3.2.3 (14-April-2017)
Voice and Unified Communications Devices		
Cisco ATA 187 Analog Telephone Adaptor	CSCvc94765	修正予定なし
Cisco Agent Desktop for Cisco Unified Contact Center Express	CSCvc94745	EoSWM (16-July-2016) 期待される修正無し
Cisco Agent Desktop	CSCvc94581	修正予定なし
Cisco Emergency Responder	CSCvc94749	CER 12.0 (July-2017)
Cisco Finesse	CSCvc98369	
Cisco Hosted Collaboration Mediation Fulfillment	CSCvc94752	
Cisco IP 7800 シリーズ電話	CSCvc94768	12.0 (31-Aug-2017)
Cisco IP 8800 シリーズ電話-VPN 機能	CSCvc94767	12.0 (12-DEC-2017)
Cisco MediaSense	CSCvc98372	11.5 SU02 (4-Aug-2017)
Cisco Unified Attendant Console Advanced	CSCvc94735	11.0.2 (3-April-2017)
Cisco Unified Attendant Console Business Edition	CSCvc94735	11.0.2 (3-April-2017)
Cisco Unified Attendant Console Department Edition	CSCvc94735	11.0.2 (3-April-2017)
Cisco Unified Attendant Console Enterprise Edition	CSCvc94735	11.0.2 (3-April-2017)
Cisco Unified Attendant Console Premium Edition	CSCvc94735	11.0.2 (3-April-2017)
Cisco Unified Communications Manager IM & Presence Service (旧称 CUPS)	CSCvc94750	
Cisco Unified Communications Manager Session Management Edition	CSCvc94740	
Cisco Unified Communications Manager	CSCvc94740	

Cisco Unified Contact Center Express	CSCvc96176	11.6(1) (30-April-2017)
Cisco Unified IP 7937 電話	CSCvc96113	修正予定なし
Cisco Unified IP 8945 電話	CSCvc96109	9.4(2)SR4 (Dec-2017)
Cisco Unity Connection	CSCvc94741	12.0: Available 11.5: Available
Cisco Virtualization Experience Media Edition	CSCvc94773	11.9 (30-June-2017)
Cisco Virtualized Voice Browser	CSCvc98374	11.6.1 (10-May-2017)

Video, Streaming, TelePresence, and Transcoding Devices

Cisco 4300 シリーズ Digital Media Player	CSCvc94651	5.4.1(RB3) (25-Feb-2017) 5.3.6(RB3) (25-Feb-2017)
Cisco 4400 シリーズ Digital Media Player	CSCvc94651	5.4.1(RB3) (25-Feb-2017) 5.3.6(RB3) (25-Feb-2017)
Cisco Cloud Object Storage	CSCvc94672	3.14.0 (30-March-2017)
Cisco Edge 300 Digital Media Player	CSCvc94710	1.6RB5_2 (01-March-2017)
Cisco Edge 340 Digital Media Player	CSCvc94713	1.2RB1.0.6 (2-March-2017)
Cisco Expressway Series	CSCvc94669	X8.9.2 (31-Mar-2017)
Cisco TelePresence Conductor	CSCvc94650	4.3.1 (29-Mar-2017)
Cisco TelePresence MX Series	CSCvc94665	CE8.3.2 (April-2017) 7.3.10 (August-2017)
Cisco TelePresence Profile Series	CSCvc94665	CE8.3.2 (April-2017) 7.3.10 (August-2017)
Cisco TelePresence SX Series	CSCvc94665	CE8.3.2 (April-2017) 7.3.10 (August-2017) 500-32 - CTS6.1.13(6) (10-April-2017) 1300 - CTS6.1.13(6) (10-April-2017) TX1310 - CTS6.1.13(6) (10-April-2017) TX9000 シリーズ- CTS6.1.13(6) (10-April-2017)
Cisco TelePresence System 1000	CSCvc94733	500-37- CTS1.10.16(4) (10-April-2017) 1000 - CTS1.10.16(4) (10-April-2017) 1100 - CTS1.10.16(4) (10-April-2017) 3000 シリーズ- CTS1.10.16(4) (10-April-2017) 500-32 - CTS6.1.13(6) (10-April-2017) 1300 - CTS6.1.13(6) (10-April-2017) TX1310 - CTS6.1.13(6) (10-April-2017) TX9000 シリーズ- CTS6.1.13(6) (10-April-2017)
Cisco TelePresence System 1100	CSCvc94733	500-37- CTS1.10.16(4) (10-April-2017) 1000 - CTS1.10.16(4) (10-April-2017) 1100 - CTS1.10.16(4) (10-April-2017) 3000 シリーズ- CTS1.10.16(4) (10-April-2017) 500-32 - CTS6.1.13(6) (10-April-2017) 1300 - CTS6.1.13(6) (10-April-2017)
Cisco TelePresence System 1300	CSCvc94733	TX1310 - CTS6.1.13(6) (10-April-2017) TX9000 シリーズ- CTS6.1.13(6) (10-April-2017)

		500-37- CTS1.10.16(4) (10-April-2017) 1000 - CTS1.10.16(4) (10-April-2017) 1100 - CTS1.10.16(4) (10-April-2017) 3000 シリーズ- CTS1.10.16(4) (10-April-2017) 500-32 - CTS6.1.13(6) (10-April-2017) 1300 - CTS6.1.13(6) (10-April-2017) TX1310 - CTS6.1.13(6) (10-April-2017) TX9000 シリーズ- CTS6.1.13(6) (10-April-2017)
Cisco TelePresence System 3000 Series	CSCvc94733	500-37- CTS1.10.16(4) (10-April-2017) 1000 - CTS1.10.16(4) (10-April-2017) 1100 - CTS1.10.16(4) (10-April-2017) 3000 シリーズ- CTS1.10.16(4) (10-April-2017) 500-32 - CTS6.1.13(6) (10-April-2017) 1300 - CTS6.1.13(6) (10-April-2017) TX1310 - CTS6.1.13(6) (10-April-2017) TX9000 シリーズ- CTS6.1.13(6) (10-April-2017)
Cisco TelePresence System 500-32	CSCvc94733	500-37- CTS1.10.16(4) (10-April-2017) 1000 - CTS1.10.16(4) (10-April-2017) 1100 - CTS1.10.16(4) (10-April-2017) 3000 シリーズ- CTS1.10.16(4) (10-April-2017) 500-32 - CTS6.1.13(6) (10-April-2017) 1300 - CTS6.1.13(6) (10-April-2017) TX1310 - CTS6.1.13(6) (10-April-2017) TX9000 シリーズ- CTS6.1.13(6) (10-April-2017)
Cisco TelePresence System 500-37	CSCvc94733	500-37- CTS1.10.16(4) (10-April-2017) 1000 - CTS1.10.16(4) (10-April-2017) 1100 - CTS1.10.16(4) (10-April-2017) 3000 シリーズ- CTS1.10.16(4) (10-April-2017)
Cisco TelePresence System EX シリーズ	CSCvc94665	CE8.3.2 (April-2017) 7.3.10 (August-2017) 500-32 - CTS6.1.13(6) (10-April-2017) 1300 - CTS6.1.13(6) (10-April-2017) TX1310 - CTS6.1.13(6) (10-April-2017) TX9000 シリーズ- CTS6.1.13(6) (10-April-2017)
Cisco TelePresence システム TX1310	CSCvc94733	500-37- CTS1.10.16(4) (10-April-2017) 1000 - CTS1.10.16(4) (10-April-2017) 1100 - CTS1.10.16(4) (10-April-2017) 3000 シリーズ- CTS1.10.16(4) (10-April-2017) 500-32 - CTS6.1.13(6) (10-April-2017) 1300 - CTS6.1.13(6) (10-April-2017) TX1310 - CTS6.1.13(6) (10-April-2017) TX9000 シリーズ- CTS6.1.13(6) (10-April-2017)
Cisco TelePresence TX9000 シ リーズ	CSCvc94733	500-37- CTS1.10.16(4) (10-April-2017)

		1000 - CTS1.10.16(4) (10-April-2017)
		1100 - CTS1.10.16(4) (10-April-2017)
		3000 シリーズ- CTS1.10.16(4) (10-April-2017)
Cisco TelePresence Video Communication Server (VCS)	CSCvc94669	X8.9.2 (31-Mar-2017)
Cisco Telepresence Integrator C	CSCvc94665	CE8.3.2 (April-2017) 7.3.10 (August-2017)
Cisco ビデオ サーベイランス 4300E および 4500E 高精細度 IP カメラ	CSCvc94689	3.2.7 240:(1 行進2017)
Cisco Video Surveillance Media Server	CSCvc94691	7.10 (eta June-2017)
Cisco Videoscape AnyRes Live	CSCvc94718	9.7.4 (14-Feb-2017)
Cisco Videoscape Voyager Vantage	CSCvc94721	有利な 6.4 r 5 つ 1 つ \n OpenSSL 1.0.2i (-May-2017)
Wireless		
Cisco Mobility Services Engine	CSCvc94636	
Ciscoワイヤレス LAN コントローラ	CSCvc94648	8.5 (March-2017)
Cisco Hosted Services		
Cisco Business Video Services Automation Software	CSCvc94560	BV-VSAA 11.x (31-Dec-2017)
Cisco Smart Care	CSCvc94677	修正予定なし
Cisco WebEx Meeting Center ciscossl	CSCvc94598 CSCvd41263	1.3.28 (30-Apr-2017)

脆弱性を含んでいないことが確認された製品

以下の製品はこのアドバイザリに説明がある脆弱性から影響を受けません。

Collaboration and Social Media

- Cisco Unified MeetingPlace
- Cisco WebEx Node for MCS

エンドポイント クライアントとクライアント ソフトウェア

- Cisco Agent for OpenFlow
- Cisco AnyConnect Secure Mobility Client for Android
- Cisco AnyConnect Secure Mobility Client for Linux
- Mac OS X のための Cisco AnyConnect セキュア モビリティ クライアント
- Cisco AnyConnect Secure Mobility Client for Windows
- Cisco AnyConnect Secure Mobility Client for iOS
- Cisco Jabber クライアント フレームワーク (JCF) コンポーネント
- Cisco Jabber for Android
- Cisco WebEx Meetings for Android
- Windows 電話 8 のための Cisco WebEx Meetings

ネットワーク アプリケーション、サービス、およびアクセラレーション

- Cisco Visual Quality Experience Server
- Cisco Visual Quality Experience Tools Server
- Cisco Wide Area Application Services (WAAS)

ネットワークおよびコンテンツ セキュリティ デバイス

- Cisco ASA Next-Generation Firewall Services
- Cisco Adaptive Security Appliance (ASA)
- Cisco Secure Access Control System (ACS)
- Cisco Virtual Security Gateway for Microsoft Hyper-V

ネットワーク管理とプロビジョニング

- Cisco Application Networking Manager
- Cisco Configuration Professional
- Cisco Digital Media Manager
- Cisco 管理 アプライアンス
- Cisco Multicast Manager
- Cisco Packet Tracer
- Cisco Policy Suite
- Cisco Prime Collaboration Provisioning
- Cisco Prime Home
- Cisco Prime Infrastructure プラグアンドプレイ スタンドアロンゲートウェイ
- Cisco Prime LAN Management Solution - Solaris
- Cisco Prime Network Registrar IP アドレス マネージャ (IPAM)
- Cisco Prime Network Services Controller
- Cisco Prime Network
- Cisco Security Manager
- Cisco UCS Central ソフトウェア
- Lancope Stealthwatch Endpoint Concentrator
- Lancope Stealthwatch FlowCollector NetFlow
- Lancope Stealthwatch FlowCollector sFlow
- Lancope Stealthwatch FlowSensor
- Lancope Stealthwatch SMC
- Lancope Stealthwatch UDP Director

ルーティングおよびスイッチング - エンタープライズおよびサービス プロバイダー

- Cisco Broadband Access Center for Telco and Wireless
- Cisco Nexus 1000V シリーズ スイッチ

- VMware vSphere 向け Cisco Nexus 1000V スイッチ
- Cisco Nexus 9000 シリーズ スイッチ (スタンドアロン、NX-OS モード)
- Cisco ONS 15454 Series Multiservice Provisioning Platforms
- Cisco Service Control Operating System

ルーティングおよびスイッチング - スモール ビジネス

- (Sx220) スイッチとスマートな Cisco 220 シリーズ
- Cisco 500 シリーズ スタック可能 (Sx500) 管理されたスイッチ
- Cisco スモール ビジネス 300 シリーズ (Sx300) はスイッチを管理しました

Unified Computing

- Cisco UCS スタンドアロン Cシリーズ ラック サーバ- Integrated Management Controller
- Cisco Virtual Security Gateway

音声およびユニファイド コミュニケーション デバイス

- Cisco ATA 190 シリーズ アナログ ターミナル アダプタ
- Cisco Computer Telephony Integration Object Server (CTIOS)
- Cisco DX シリーズ IP フォン
- Cisco IP Interoperability and Collaboration System (IPICS)
- Cisco Packaged Contact Center Enterprise
- Cisco Paging Server (Informacast)
- Cisco Paging Server
- Cisco SPA112 2-Port Phone Adapter
- ルータとの Cisco SPA122 Analog Telephone Adapter (ATA)
- Cisco SPA232D マルチライン DECT Analog Telephone Adapter (ATA)
- Cisco SPA51x IP フォン
- Cisco SPA525G 5 行 IP Phone
- Cisco Small Business SPA300 シリーズ IP Phone
- Cisco Small Business SPA500 シリーズ IP Phone
- Cisco TAPI Service Provider (TSP)
- Cisco UC Integration for Microsoft Lync
- Cisco Unified Attendant Console Standard
- Cisco Unified Communications Domain Manager
- Cisco Unified Contact Center Enterprise
- Cisco Unified IP 6901 電話
- Cisco Unified IP 6945 電話
- Cisco Unified IP 7900 シリーズ電話
- サードパーティ コール制御のための Cisco Unified IP 8831 会議電話
- Cisco Unified IP 8831 会議電話

- Cisco Unified IP 8961 電話
- Cisco Unified IP 9951 電話
- Cisco Unified IP 9971 電話
- Cisco Unified Intelligent Contact Management Enterprise
- Cisco Unified SIP Proxy ソフトウェア
- Cisco Unified Wireless IP Phone
- Cisco Unified Workforce Optimization
- Cisco Unity Express

ビデオ、ストリーミング、テレプレゼンス、およびトランスコーディング デバイス

- Cisco DCM シリーズ D990x デジタル コンテンツ マネージャ
- Cisco Enterprise Content Delivery System (ECDS)
- Cisco MXE 3500 Series Media Experience Engines
- Cisco TelePresence Content Server
- Cisco TelePresence ISDN Gateway 3241
- Cisco TelePresence ISDN Gateway MSE 8321
- Cisco TelePresence ISDN Link
- Cisco TelePresence MCU 4200 シリーズ、4500 シリーズ、5300 シリーズ、MSE 8420、および MSE 8510
- Cisco TelePresence Serial Gateway Series
- Cisco TelePresence Server 7010 および MSE 8710
- 複数政党制メディア 310 および 320 の Cisco TelePresence Server
- 複数政党制メディア 820 の Cisco TelePresence Server
- Cisco TelePresence Server on Virtual Machine
- Cisco TelePresence Supervisor MSE 8050
- Cisco Video Distribution Suite for Internet Streaming (VDS-IS/CDS-IS)
- Cisco Video Surveillance 3000 Series IP Cameras
- Cisco Video Surveillance 4000 Series High-Definition IP Cameras
- Cisco Video Surveillance 6000 Series IP Cameras
- Cisco Video Surveillance 7000 Series IP Cameras
- Cisco Video Surveillance PTZ IP Cameras
- Cisco Videoscape Control Suite
- Tandberg Codian ISDN ゲートウェイ 3210、3220、および 3240
- Tandberg Codian MSE 8320

ワイヤレス

- Cisco Aironet 1040 シリーズ
- Cisco Aironet 1130 AG シリーズ
- Cisco Aironet 1140 シリーズ
- Cisco Aironet 1200 シリーズ

- Cisco Aironet 1530 シリーズ
- Cisco Aironet 1550 シリーズ
- Cisco Aironet 1570 シリーズ
- Cisco Aironet 1600 シリーズ
- Cisco Aironet 1700 シリーズ
- Cisco Aironet 2600 シリーズ
- Cisco Aironet 2700 シリーズ
- Cisco Aironet 3500 シリーズ
- Cisco Aironet 3600 シリーズ
- Cisco Aironet 3700 シリーズ
- Cisco Aironet 700 シリーズ
- Cisco Aironet 700W シリーズ
- Cisco Industrial Wireless 3700 シリーズ

シスコ ホステッド サービス

- ネットワーク認証のための Cisco 査定 サービス
- Cisco Cloud Web Security
- Cisco クラウドおよびシステム管理
- Cisco Network Device Security Assessment Service
- Cisco ネットワーク健全性フレームワーク
- Cisco Network Performance Analysis
- Cisco One Portal
- Cisco Partner Support Service 1.x
- Cisco Prime Network 変更および設定管理
- Cisco Proactive Network Operations Center
- Cisco Registered Envelope Service
- Cisco Services Provisioning Platform
- Cisco Smart Net Total Care - Contracts Information System Process Controller
- Cisco Smart Net Total Care -スマートな相互対話
- Cisco Smart Net Total Care
- Cisco Unified Service Delivery プラットフォーム
- Cisco Universal Small Cell 5000 シリーズ-リリース 3.4.2.x の実行
- Cisco Universal Small Cell 7000 シリーズ-リリース 3.4.2.x の実行
- Cisco ユニバーサル小さいセル CloudBase ファクトリ リカバリ ルート ファイルシステム-リリース 2.99.4 およびそれ以降
- Cisco ユニバーサル小さいセル Iuh
- Cisco WebEx Messenger Service

詳細

OpenSSL はサービス拒否の脆弱性を処理するパケットを切捨てました

OpenSSL の脆弱性はリモート攻撃者非認証によりサービス拒否 (DoS) 状態を引き起こすようにする可能性があります。

脆弱性はシステムが特定の暗号を使用しているとき影響を受けた 32ビット上位 システムの切捨てられたパケットの不適切な処理が原因です。 攻撃者はターゲットのシステムへ切捨てられたパケットを送信 することによってこの脆弱性を不正利用する可能性があります。 エクスプロイトは読まれたの境界調節しま引き起こし、DoS 状態に終ってクラッシュするためにシステムを引き起こします。

OpenSSL 鍵交換処理サービス拒否の脆弱性

OpenSSL の脆弱性はリモート攻撃者非認証によりサービス拒否 (DoS) 状態を引き起こすようにする可能性があります。

脆弱性は影響を受けたソフトウェアによって処理されるユーザが指定する入力の不十分な検証が原因です。 攻撃者は悪意のあるサーバの Diffie-Hellmanキー交換 (DHE) または楕円曲線 DHE (ECDHE) およびクライアント システムのターゲットとされたユーザを悪意のあるサーバと通信するように説得することのために巧妙に細工された パラメータを入れるように設計されている使用によってこの脆弱性を不正利用する可能性があります。 エクスプロイトはクライアント システムの可能性があります、クラッシュするためにシステムをおよび DoS 状態に終るヌルポイント参照解除条件を引き起こします引き起こす。

情報漏洩の脆弱性を平方する OpenSSL モントゴメリー

OpenSSL の脆弱性はリモート攻撃者非認証がターゲットのシステムの機密情報にアクセスするようにする可能性があります。

脆弱性は影響を受けたソフトウェアのプロシージャを平方する x86_64 モントゴメリーにあります。 攻撃者はパッチ設定されていないシステムにオンライン アクセスの設定される Diffie-Hellman (DH) パラメータと共用プライベートキーを使用する取得によってこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者が敏感な秘密キーの情報にアクセスすることを可能にする可能性があります。

OpenSSL ハンドシェイク ネゴシエーション サービス拒否の脆弱性

OpenSSL の脆弱性はリモート攻撃者非認証によりターゲットのシステムのサービス拒否 (DoS) 条件を引き起こすようにする可能性があります。

脆弱性は影響を受けたソフトウェアによって不適切な保安検査が原因です。 攻撃者は影響を受けたソフトウェアによって再ネゴシエーション ハンドシェイクの間にこの脆弱性を不正利用する可

能性があります。暗号化 Mac 拡張がハンドシェイクの間にネゴシエートされる場合、システムはターゲットのシステムの DoS 条件に終って、適切に機能することを止める可能性があります。

回避策

回避策は利用可能になり次第、Cisco Bugs に記載されます。バグは [Cisco Bug Search Tool](#) で検索できます。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。

<http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN.html>

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限りです。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する場合は、<http://www.cisco.com/go/psirt> の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成は新規リリースでも継続して適切なサポートが受けられることを確認してください。不明な点については、Cisco Technical Assistance Center (TAC) もしくは契約しているメンテナンス プロバイダーにお問い合わせください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center (TAC) に連絡してアップグレードを入手してください。

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

各脆弱なプロダクトのための影響を受けたのおよび修正済みリソースを判別するために、このアドバイザリの「脆弱性が存在する製品」セクションの製品のために識別される Cisco バグを参照して下さい。Cisco Bugs は、[Cisco Bug Search Tool](#) で検索できます。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) では、本アドバイザリに記載されている脆弱性の不正利用事例とその公表は確認しておりません。

OpenSSL 鍵交換処理サービス拒否の脆弱性のために存在する公共エクスプロイト CVE-2017-3730。

出典

これらの脆弱性は OpenSSL ソフトウェア基礎によって公に [2017 年 1 月 26 日](#) および [2017 年 2 月 16 日](#) 表われました。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170130-openssl>

改訂履歴

Version	Description	Section	Status	日付
2.9	未知数にこの段階でアップデートされる MSE 修正。	脆弱性のある製品	Final	2017-July-05
2.8	追加された Cisco IOS XR 最初修正済みリリース。	脆弱性のある製品	Final	2017-June-20
2.7	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Final	2017-April-27
2.6	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-April-14
2.5	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-April-07
2.4	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-March-31
2.3	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-March-23
2.2	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-March-10
2.1	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-March-01

			m	
2.0	OpenSSL 基礎によつての 2017 年 2 月第 16 表われる新しい脆弱性が含まれる更新済要約。該当製品のための更新済製品リスト。	要約、該当製品、脆弱性が存在する製品、脆弱性が存在しない製品、出典	Interim	2017-February-17
1.1	Updated product lists.	Affected Products, Vulnerable Products, Products Confirmed Not Vulnerable	Interim	2017-February-03
1.0	初回公開リリース		Interim	2017-January-30

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。