シスコ製品に影響を与えるOpenSSLの複数の脆弱性：2017年1月および2月

Medium

アドバイザリーID : cisco-sa-20170130-openssl
初公開日 : 2017-01-30 21:28
最終更新日 : 2017-07-05 11:43
バージョン 2.9 : Final
回避策 : No workarounds available
Cisco バグ ID : CSCvc94616 CSCvc94581 CSCvc94585 CSCvc94662 CSCvc94665 CSCvc94589 CSCvc94741 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

CVE-2017-3730 CVE-2017-3732 CVE-2017-3731 CVE-2017-3733

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、OpenSSL Software Foundationは、新しい3つの脆弱性を含むセキュリティアドバイザリをリリースしました。また、2016年11月にOpenSSLアドバイザリで公開済みで、Cisco Security Advisory『Multiple Vulnerabilities in OpenSSL Affecting Cisco Products: November 2016』に含まれている脆弱性が1つリリースされました。OpenSSLでは、すべての新しい脆弱性が「中程度の重大度」に分類されます。

1つ目の脆弱性は、32ビットシステムアーキテクチャで使用されているOpenSSLにのみ影響し、OpenSSLがクラッシュする原因となる可能性があります。2つ目の脆弱性は、バージョン1.1.0のみに影響し、クライアント側でOpenSSLが使用されている場合にのみ発生します。2つ目の脆弱性は、悪意のあるサーバに接続したときにOpenSSLがクラッシュする原因となる可能性があります。3つ目の脆弱性は、x86_64アーキテクチャに基づくシステムにのみ影響します。3番目の脆弱性の不正利用に成功すると、攻撃者は秘密キーの機密情報にアクセスできる可能性があります。

複数のシスコ製品に、これらの脆弱性の1つ以上の影響を受けるバージョンのOpenSSLパッケージが組み込まれています。

CVE ID CVE-2017-3730で特定された脆弱性の影響を受けるシスコ製品はありません。

2017年2月16日、OpenSSL Software Foundationは、CVE ID CVE-2017-3733で識別される重大度の高い脆弱性を含む別のセキュリティアドバイザリをリリースしました。

この脆弱性の影響を受けるシスコ製品はありません。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.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。製品が影響を受けるかどうかを確認するには、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」の項を参照してください。

「脆弱性のある製品」セクションで、影響を受ける各製品のCisco Bug IDを示します。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によって特定された脆弱性の影響を受けるシスコ製品はありません。

脆弱性のある製品

製品	Cisco Bug ID	Fixed Release Availability
Collaboration and Social Media		
Cisco SocialMiner	CSCvc98364	
Cisco WebEx Meetings Serverリリース1.x	CSCvc94595	CWMS 2.8（2017年3月31日）
Cisco WebEx Meetings Serverリ	CSCvc94595	CWMS 2.8（2017年3月31日）

リース2.x		
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 Jabber Guest	CSCvc94762	11.0(1)（2017年5月31日）
Cisco Jabber Software Development Kit	CSCvc94759	11.9（2017年6月30日）
Cisco Jabber for Mac	CSCvc94758	11.9（2017年6月30日）
Cisco Jabber for Windows	CSCvc94760	11.9.0（2017年6月28日）
Cisco Webex Business Suite	CSCvc94597	NBR 3.6.0（2017年3月30日）
Cisco Webex Meetings Client - ホスト型	CSCvc96091	31.12（2017年2月28日）
Cisco WebEx Meetingsクライアント – オンプレミス	CSCvc96090	31.12（2017年2月28日）
Cisco WebEx Meetings Server – マルチメディアプラットフォーム (MMP)	CSCvc96092	6.0.325（入手可能）
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コンテンツセキュリティアプライアンスアップデートサーバ	CSCvc94591	2.0.3-111（2017年3月3日）
Cisco Content Security Management Appliance (SMA)	CSCvc94590	11.5（2017年9月）
Cisco Email Security Appliance (ESA)	CSCvc94585	11.5（2017年9月）
Cisco FireSIGHT システム ソフトウェア	CSCvc94589	6.2.0.1（2017年4月）6.1.0.3（2017年7月）6.0.1.3（2017年6月）5.4.0.11/5.4.1.10（2017年7月）
Cisco Identity Services Engine（ISE）	CSCvc94692	
Cisco Web Security Appliance (WSA)	CSCvc94592	11.5（2017年9月）
ネットワーク管理とプロビジョニング		
Cisco Application Policy Infrastructure Controller（APIC）	CSCvc96095	2.3（2017年6月）
Cisco MATE Collector	CSCvc94716	
Cisco MATE Design	CSCvc94716	
Cisco MATE Live	CSCvc94716	
Cisco NetFlow Generation	CSCvc94643	1.1.1（2017年4月13日）

Appliance		1.1.1a（2017年4月13日）
Cisco Network Analysis Module	CSCvc94637	6.2.1（2017年4月13日） 6.2.2（2017年4月13日）
Cisco Prime Access Registrar	CSCvc94632	8.0（2017年7月30日）
Cisco Prime Collaboration Assurance	CSCvc96099	PCA 11.6で修正済み
Cisco Prime Collaboration Deployment	CSCvc96106	
Cisco Prime Data Centerネットワークマネージャ	CSCvc94601	10.2.1（2017年4月21日）
Cisco Prime IP Express	CSCvc94634	8.3.5（2017年2月28日）
Cisco Prime Infrastructure	CSCvc94641	3.2:（2017年3月31日） 3.1.6（2017年3月31日）
Cisco Prime License Manager	CSCvc94662	11.5 (1.12001-2) (2017年4月7日
Cisco Prime Network Registrar	CSCvc94629	8.3.5（2017年2月28日）
Cisco Prime Opticalサービス プロバイダー向け	CSCvc94633	10.6.1.0（2017年2月）
Cisco Prime Performance Manager	CSCvc94623	SP1703（2017年3月31日）
Cisco Smart Net Total Care - ローカル コレクタ アプライアンス	CSCvc94723	2.2.14（2017年2月10日）
Cisco Unified Intelligence Center	CSCvc98361	
Routing and Switching - Enterprise and Service Provider		
Cisco ASR 5000 シリーズ	CSCvc94556	21.2.0（2017年4月30日）
Cisco Application Policy Infrastructure Controller（APIC）	CSCvc94602	2.3（2017年7月）
Cisco Connected Grid ルータ	CSCvc94730	15.6(3)M2（2017年3月31日）
Cisco IOS XR ソフトウェア	CSCvc94649	6.3.1
Cisco IOS ソフトウェアおよびCisco IOS XE ソフトウェア	CSCvc94729	16.6（2017年2月15日）
Cisco MDS 9000 Series Multilayer Switches	CSCvc94605	6.2.21利用可能な修正がまだない 8.2.1（2017年9月）7.0.3.I6（2017年3月）
Cisco MDS 9000 Series Multilayer Switches	CSCvc94606	MDS 9000:6.2.21まだ修正プログラムはない 5,000ナイラ N6K：修正予定なし

		N7K:8.2.1（2017年9月） N3K N9K 7.0.3.I6（2017年4月）
Cisco Nexus 1000V InterCloud	CSCvc94604	修正予定なし
Cisco Nexus 3000 Series Switches	CSCvc94609	6.0(2)A8(4)（2017年4月15日）
Cisco Nexus 4000 Series Blade Switches	CSCvc94709	4.1(2)E1(1s)（2017年7月15日）
Cisco Nexus 5000 Series Switches	CSCvc94606	MDS 9000:6.2.21まだ修正プログラムはない 5,000ナイラ N6K：修正予定なし N7K:8.2.1（2017年9月） N3K N9K 7.0.3.I6（2017年4月）
Cisco Nexus 5000 Series Switches	CSCvc94610	7.3（2017年5月2日）
Cisco Nexus 6000 Series Switches	CSCvc94606	MDS 9000:6.2.21まだ修正プログラムはない 5,000ナイラ N6K：修正予定なし N7K:8.2.1（2017年9月） N3K N9K 7.0.3.I6（2017年4月）
Cisco Nexus 7000 Series Switches	CSCvc94606	MDS 9000:6.2.21まだ修正プログラムはない 5,000ナイラ N6K：修正予定なし N7K:8.2.1（2017年9月） N3K N9K 7.0.3.I6（2017年4月）
Cisco Nexus 9000 シリーズ ファブリック スイッチ（ACI モード）	CSCvc94603	12.3x Drava（2017年6月）
Unified Computing		
Cisco Common Services Platform Collector	CSCvc94568	CASP 1.12（2017年3月10日）
Cisco UCS 6200シリーズおよび6300シリーズファブリックイン	CSCvc94686	3.2.3（2017年4月14日）

ターコネクト		
Cisco UCS Bシリーズブレードサーバ	CSCvc94616	3.2（2017年6月）
Cisco UCS Director	CSCvc96093	6.1 GlacierBay（2017年5月31日）
Cisco UCS Manager	CSCvc96103	3.2.3（2017年4月14日）
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 187 Analog Telephone Adaptor	CSCvc94765	修正予定なし
Cisco Agent Desktop for Cisco Unified Contact Center Express	CSCvc94745	EoSWM（2016年7月16日）修正予定なし
Cisco Agent Desktop	CSCvc94581	修正予定なし
Cisco Emergency Responder	CSCvc94749	CER 12.0（2017年7月）
Cisco Finesse	CSCvc98369	
Cisco Hosted Collaboration Mediation Fulfillment	CSCvc94752	
Cisco IP 7800シリーズ電話機	CSCvc94768	12.0（2017年8月31日）
Cisco IP 8800シリーズPhone - VPN機能	CSCvc94767	12.0（2017年12月12日）
Cisco MediaSense	CSCvc98372	11.5 SU02（2017年8月4日）
Cisco Unified Attendant Console Advanced	CSCvc94735	11.0.2（2017年4月3日）
Cisco Unified Attendant Console Business Edition	CSCvc94735	11.0.2（2017年4月3日）
Cisco Unified Attendant Console Department Edition	CSCvc94735	11.0.2（2017年4月3日）
Cisco Unified Attendant Console Enterprise Edition	CSCvc94735	11.0.2（2017年4月3日）
Cisco Unified Attendant Console Premium Edition	CSCvc94735	11.0.2（2017年4月3日）
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)（2017年4月30日）
Cisco Unified IP 7937電話	CSCvc96113	修正予定なし
Cisco Unified IP 8945電話	CSCvc96109	9.4(2)SR4（2017年12月）
Cisco Unity Connection	CSCvc94741	12.0：利用可能 11.5：利用可能
Cisco Virtualization Experience Media Edition	CSCvc94773	11.9（2017年6月30日）
Cisco Virtualized Voice Browser	CSCvc98374	11.6.1（2017年5月10日）
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 4300シリーズデジタルメディアプレーヤー	CSCvc94651	5.4.1(RB3)（2017年2月25日）5.3.6(RB3)（2017年2月25日）
Cisco 4400シリーズデジタルメディアプレーヤー	CSCvc94651	5.4.1(RB3)（2017年2月25日）5.3.6(RB3)（2017年2月25日）
Cisco Cloud Object Storage	CSCvc94672	3.14.0（2017年3月30日）
Cisco Edge 300 Digital Media Player	CSCvc94710	1.6RB5_2（2017年3月1日）
Cisco Edge 340 Digital Media Player	CSCvc94713	1.2RB1.0.6（ 2017年3月2日）
Cisco Expressway Series	CSCvc94669	X8.9.2（2017年3月31日）
Cisco TelePresence Conductor	CSCvc94650	4.3.1（2017年3月29日）
Cisco TelePresence MX Series	CSCvc94665	CE8.3.2（2017年4月） 7.3.10（2017年8月）
Cisco TelePresence Profile Series	CSCvc94665	CE8.3.2（2017年4月） 7.3.10（2017年8月）
Cisco TelePresence SX Series	CSCvc94665	CE8.3.2（2017年4月） 7.3.10（2017年8月）
Cisco TelePresence System 1000	CSCvc94733	500-32 - CTS6.1.13(6)（2017年4月10日） 1300 - CTS6.1.13(6)（2017年4月10日） TX1310 - CTS6.1.13(6)（2017年4月10日） TX9000シリーズ – CTS6.1.13(6)（2017年4月10日） 500-37- CTS1.10.16(4)（2017年4月10日） 1000 - CTS1.10.16(4)（2017年4月10日） 1100 - CTS1.10.16(4)（2017年4月10日） 3000シリーズ – CTS1.10.16(4)（2017年4月10日）

Cisco TelePresence System 1100	CSCvc94733	500-32 - CTS6.1.13(6)（2017年4月10日） 1300 - CTS6.1.13(6)（2017年4月10日） TX1310 - CTS6.1.13(6)（2017年4月10日） TX9000シリーズ – CTS6.1.13(6)（2017年4月10日） 500-37- CTS1.10.16(4)（2017年4月10日） 1000 - CTS1.10.16(4)（2017年4月10日） 1100 - CTS1.10.16(4)（2017年4月10日） 3000シリーズ – CTS1.10.16(4)（2017年4月10日）
Cisco TelePresence System 1300	CSCvc94733	500-32 - CTS6.1.13(6)（2017年4月10日） 1300 - CTS6.1.13(6)（2017年4月10日） TX1310 - CTS6.1.13(6)（2017年4月10日） TX9000シリーズ – CTS6.1.13(6)（2017年4月10日） 500-37- CTS1.10.16(4)（2017年4月10日） 1000 - CTS1.10.16(4)（2017年4月10日） 1100 - CTS1.10.16(4)（2017年4月10日） 3000シリーズ – CTS1.10.16(4)（2017年4月10日）
Cisco TelePresence System 3000 Series	CSCvc94733	500-32 - CTS6.1.13(6)（2017年4月10日） 1300 - CTS6.1.13(6)（2017年4月10日） TX1310 - CTS6.1.13(6)（2017年4月10日） TX9000シリーズ – CTS6.1.13(6)（2017年4月10日） 500-37- CTS1.10.16(4)（2017年4月10日） 1000 - CTS1.10.16(4)（2017年4月10日） 1100 - CTS1.10.16(4)（2017年4月10日） 3000シリーズ – CTS1.10.16(4)（2017年4月10日）
Cisco TelePresence System 500-32	CSCvc94733	500-32 - CTS6.1.13(6)（2017年4月10日） 1300 - CTS6.1.13(6)（2017年4月10日） TX1310 - CTS6.1.13(6)（2017年4月10日） TX9000シリーズ – CTS6.1.13(6)（2017年4月10日） 500-37- CTS1.10.16(4)（2017年4月10日） 1000 - CTS1.10.16(4)（2017年4月10日）

		1100 - CTS1.10.16(4)（2017年4月10日） 3000シリーズ – CTS1.10.16(4)（2017年4月10日）
Cisco TelePresence System 500-37	CSCvc94733	500-32 - CTS6.1.13(6)（2017年4月10日） 1300 - CTS6.1.13(6)（2017年4月10日） TX1310 - CTS6.1.13(6)（2017年4月10日） TX9000シリーズ – CTS6.1.13(6)（2017年4月10日） 500-37- CTS1.10.16(4)（2017年4月10日） 1000 - CTS1.10.16(4)（2017年4月10日） 1100 - CTS1.10.16(4)（2017年4月10日） 3000シリーズ – CTS1.10.16(4)（2017年4月10日）
Cisco TelePresence System EX シリーズ	CSCvc94665	CE8.3.2（2017年4月） 7.3.10（2017年8月）
Cisco TelePresenceシステム TX1310	CSCvc94733	500-32 - CTS6.1.13(6)（2017年4月10日） 1300 - CTS6.1.13(6)（2017年4月10日） TX1310 - CTS6.1.13(6)（2017年4月10日） TX9000シリーズ – CTS6.1.13(6)（2017年4月10日） 500-37- CTS1.10.16(4)（2017年4月10日） 1000 - CTS1.10.16(4)（2017年4月10日） 1100 - CTS1.10.16(4)（2017年4月10日） 3000シリーズ – CTS1.10.16(4)（2017年4月10日）
Cisco TelePresence TX9000 シリーズ	CSCvc94733	500-32 - CTS6.1.13(6)（2017年4月10日） 1300 - CTS6.1.13(6)（2017年4月10日） TX1310 - CTS6.1.13(6)（2017年4月10日） TX9000シリーズ – CTS6.1.13(6)（2017年4月10日） 500-37- CTS1.10.16(4)（2017年4月10日） 1000 - CTS1.10.16(4)（2017年4月10日） 1100 - CTS1.10.16(4)（2017年4月10日） 3000シリーズ – CTS1.10.16(4)（2017年4月10日）
Cisco TelePresence Video Communication Server（VCS）	CSCvc94669	X8.9.2（2017年3月31日）

Cisco Telepresence Integrator C シリーズ	CSCvc94665	CE8.3.2（2017年4月） 7.3.10（2017年8月）
Cisco Video Surveillance 4300E/4500E High-Definition IP Cameras	CSCvc94689	3.2.7-240:（2017年3月1日）
Cisco Video Surveillance Media Server	CSCvc94691	7.10（eta、2017年6月）
Cisco Videoscape AnyResライブ	CSCvc94718	9.7.4 （2017年2月14日）
Cisco Videoscape Voyager Vantage	CSCvc94721	Vantage 6.4 5 1 r\n OpenSSL 1.0.2i（–2017年5月）
ワイヤレス		
Cisco Mobility Services Engine	CSCvc94636	
Cisco ワイヤレス LAN コントローラ	CSCvc94648	8.5 （2017年3月）
シスコ ホステッド サービス		
Cisco Business Video Services Automation Software	CSCvc94560	BV-VSAA 11.x（2017年12月31日）
Cisco Smart Care	CSCvc94677	修正予定なし
Cisco WebEx Meeting Center	CSCvc94598	1.3.28（2017年4月30日）
CiscoSSL	CSCvd41263	

脆弱性を含んでいないことが確認された製品

次の製品は、このアドバイザリに記載されている脆弱性の影響を受けません。

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
- Cisco AnyConnect Secure Mobility Client for Mac OS X
- Cisco AnyConnect Secure Mobility Client for Windows
- Cisco AnyConnect Secure Mobility Client for iOS

- Cisco Jabber Client Framework(JCF)のコンポーネント
- Cisco Jabber for Android
- Cisco WebEx Meetings for Android
- Cisco WebEx Meetings for Windows Phone 8

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

Routing and Switching - Enterprise and Service Provider

- 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

- Cisco 220シリーズSmart Plus(Sx220)スイッチ
- Cisco 500シリーズスタッカブル(Sx500)マネージドスイッチ
- Cisco Small Business 300シリーズ(Sx300)マネージドスイッチ

Unified Computing

- Cisco UCS スタンドアロン C シリーズ ラック サーバ - 統合管理コントローラ
- 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
- Cisco SPA122アナログ電話アダプタ(ATA)およびルータ
- Cisco SPA232D Multi-Line DECTアナログ電話アダプタ(ATA)
- Cisco SPA51x IPフォン
- Cisco SPA525G 5回線IP電話
- 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シリーズ電話機
- サードパーティ コール制御向け Cisco Unified IP 8831 Conference Phone
- Cisco Unified IP 8831会議用電話機
- 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 Series D990x Digital Content Manager
- Cisco Enterprise Content Delivery System (ECDS)
- Cisco MXE 3500 Series Media Experience Engines
- Cisco TelePresenceコンテンツサーバ
- 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
- Cisco TelePresence Server on Multiparty Media 310および320
- Cisco TelePresence Server on Multiparty Media 820
- 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 Gateway 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シスコアセスメントサービス
- Cisco Cloud Web Security
- シスコのクラウドおよびシステム管理
- Cisco Network Device Security Assessment Service
- Cisco Network Healthフレームワーク
- Cisco Network Performance Analysis
- Cisco One Portal
- Cisco Partner Support Service 1.x
- Cisco Network Configuration and Change Management
- 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 – スマートインタラクション

- 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が稼働
- Cisco Universal Small Cell 7000シリーズ：リリース3.4.2.xが稼働
- Cisco Universal Small Cell CloudBase Factory Recovery Root Filesystem：リリース2.99.4以降
- Cisco UniversalスモールセルIuh
- Cisco WebEx Messenger Service

詳細

OpenSSLでパケットが切り捨てられる処理でのDoS脆弱性

OpenSSL の脆弱性により、認証されていないリモート攻撃者がサービス妨害（DoS）状態を発生させる可能性があります。

この脆弱性は、システムが特定の暗号を使用している場合に、該当する32ビットホストシステムで切り捨てられたパケットが不適切に処理されることに起因します。攻撃者は、切り捨てられたパケットをターゲットシステムに送信することにより、この脆弱性を不正利用する可能性があります。この不正利用により、範囲外の読み取り状態が引き起こされ、システムがクラッシュしてDoS状態が発生する可能性があります。

OpenSSLキー交換の処理におけるDoS脆弱性

OpenSSL の脆弱性により、認証されていないリモート攻撃者がサービス妨害（DoS）状態を発生させる可能性があります。

この脆弱性は、該当ソフトウェアで処理されるユーザ入力の検証が不十分であることに起因します。攻撃者は、Diffie-Hellman Key Exchange(DHE)または楕円曲線DHE(ECDHE)の巧妙に細工されたパラメータを送信するように設計された悪意のあるサーバを使用し、悪意のあるサーバと通信するようにクライアントシステム上のターゲットユーザを誘導することで、この脆弱性を不正利用する可能性があります。この不正利用により、クライアントシステムでNULLポインタ参照解除状態が引き起こされ、システムがクラッシュしてDoS状態が発生する可能性があります。

OpenSSLモンゴメリの垂直化における情報漏えいの脆弱性

OpenSSLの脆弱性により、認証されていないリモートの攻撃者がターゲットシステムの機密情報にアクセスできる可能性があります。

この脆弱性は、該当ソフトウェアのx86_64 Montgomeryスク工アリング手順にあります。攻撃者

は、Diffie-Hellman(DH)パラメータが設定された共有秘密キーを使用するパッチ未適用のシステムにオンラインでアクセスすることで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は秘密キーの機密情報にアクセスでき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におけるDoS脆弱性

OpenSSL の脆弱性により、認証されていないリモートの攻撃者が、該当システムでサービス妨害（DoS）状態を発生させる可能性があります。

この脆弱性は、影響を受けるソフトウェアによる不適切なセキュリティチェックに起因します。攻撃者は、該当ソフトウェアによる再ネゴシエーションハンドシェイク中に、この脆弱性を不正利用する可能性があります。ハンドシェイク中にEncrypt-Then-Mac拡張がネゴシエートされると、システムが適切に機能しなくなり、ターゲットシステムでDoS状態が発生す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リリースしています。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、アクセスまたはその他の方法で使用した場合、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ます。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/c/ja_jp/support/web/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。

脆弱性が存在する各製品の影響を受けるリリースと修正済みリリースを確認するには、このアドバイザリの「脆弱性が存在する製品」の項で製品を識別するCisco Bugを参照してください。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エクスプロイト事例とその公表は確認しておりません。

OpenSSLキーエクスチェンジ(IKE)処理におけるDoS脆弱性、CVE-2017-3730が不正利用されます。

出典

これらの脆弱性は、 2017年1月26日および 2017年2月16日にOpenSSL Software Foundationによって公開されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170130-openssl

改訂履歴

バージョン	説明	セクション	ステータス	日付
2.9	この段階で、MSE修正が不明に更新されました。	脆弱性が存在する製品	Final	2017 年 7 月 5 日

バージョン	説明	セクション	ステータス	日付
2.8	Cisco IOS XRの最初の修正リリースを追加。	脆弱性が存在する製品	Final	2017年6月20日
2.7	製品リストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品	Final	2017年4月27日
2.6	製品リストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品	Interim	2017年4月14日
2.5	製品リストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品	Interim	2017年4月7日
2.4	製品リストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品	Interim	2017年3月31日
2.3	製品リストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品	Interim	2017年3月23日
2.2	製品リストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品	Interim	2017年3月10日
2.1	製品リストを更新。	該当製品, 脆弱性が存在する製品, 脆弱性を含んでいないことが確認された製品	Interim	2017年3月1日
2.0	2017年2月16日にOpenSSL Foundationによって公開された新しい脆弱性を含むように更新されました。該当製品の製品リストを更新。	概要、該当製品、脆弱性が存在する製品、脆弱性を含んでいないことが確認された製品、ソース	Interim	2017年2月17日
1.1	製品リストを更新。	該当製品, 脆弱性が存在	Interim	2017年

バージョン	説明	セクション	ステータス	日付
		する製品, 脆弱性を含んでいないことが確認された製品		2月3日
1.0	初回公開リリース	—	Interim	2017 年 1 月 30 日

利用規約

本アドバイザリ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。 本アドバイザリ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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。