シスコ製品に影響を与えるOpenSSLの複数の脆弱性：2016年3月

Medium

アドバイザリーID : cisco-sa-20160302-openssl
初公開日 : 2016-03-02 12:30
最終更新日 : 2016-05-23 14:04
バージョン 2.2 : Interim
回避策 : No workarounds available
Cisco バグ ID : CSCuy54659 CSCuy54539 CSCuy54536 CSCuy54657 CSCuy54537 CSCuy54534 CSCuy54655 CSCuy54535 CSCuy54665 CSCuy54541 CSCuy54662 CSCuy54542 CSCuy54660 CSCuy54540 CSCuy54549 CSCuy54547 CSCuy54668 CSCuy54545 CSCuy54546 CSCuy54433 CSCuy54676 CSCuy54674 CSCuy54551 CSCuy54672 CSCuy62564 CSCuy54558 CSCuy54679 CSCuy54436 CSCuy54687 CSCuy54564 CSCuy74294 CSCuy74297 CSCuy54560 CSCuy74298 CSCuy58091 CSCuy58090 CSCuy54569 CSCuy54567 CSCuy54600 CSCuy54688 CSCuy54601 CSCuy54455 CSCuy54576 CSCuy54577 CSCuy54453 CSCuy54575 CSCuy54696 CSCuy54451 CSCuy54452 CSCuy58096 CSCuy58094 CSCuy54616 CSCuy54457 CSCuy54611 CSCuy54458 CSCuy54579 CSCuy54612 CSCuy54587 CSCuy54500 CSCuy54585 CSCuy54465 CSCuy54586 CSCuy54463 CSCuy54584 CSCuy54460 CSCuy54580 CSCuy54628 CSCuy54508 CSCuy54505 CSCuy54626 CSCuy54506 CSCuy53654 CSCuy54504 CSCuy54502 CSCuy54623 CSCuy54510 CSCuy54631 CSCuy54478 CSCuy54599 CSCuy54630 CSCuy54473 CSCuy54474 CSCuy54595 CSCuy54472 CSCuy54518 CSCuy54639 CSCuy54516 CSCuy54637 CSCuy54517 CSCuy54514 CSCuy54636 CSCuy53668

CVE-2016-0800
CVE-2016-0799
CVE-2016-0798
CVE-2016-0797
CVE-2016-2842
CVE-2016-0705
CVE-2016-0704
CVE-2016-0703
CVE-2016-0702

CSCuy54479 CSCuy54512 CSCuy54513
CSCuy54488 CSCuy54521 CSCuy54522
CSCuy54640 CSCuy54520 CSCuy54485
CSCuy54529 CSCuy54527 CSCuy54525
CSCuy54646 CSCuy58728 CSCuy58727
CSCuy54524 CSCuy54645 CSCuy54499
CSCuy54532 CSCuy54533 CSCuy54654
CSCuy54652 CSCuy59818 CSCuy54492

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

2016年3月1日、OpenSSL Software Foundation(OSSL)は、7つの脆弱性を詳述したセキュリティアドバイザリと、 Decrypting RSA with Obsolete and Weaked eCryption(DROWN)攻撃と呼ばれる新しい攻撃をリリースしました。合計8つのCommon Vulnerabilities and Exposures(CVE)が割り当てられました。8つのCVEのうち、3つはDROWN攻撃に関連しています。残りのCVEでは、重大度の低い脆弱性が追跡されます。

DROWNは、SSLバージョン2(SSLv2)の脆弱性をアクティブに不正利用し、パッシブに収集されたTransport Layer Security(TLS)セッションを復号化するクロスプロトコル攻撃です。DROWNは、TLSプロトコルの脆弱性やプロトコルの特定の実装を不正利用しません。

DROWN攻撃を成功させるには、攻撃者はSSLv2とTLSの両方をサポートし、両方のプロトコルに同じRSAキーペアを使用するサーバを特定する必要があります。攻撃者は、サーバのTLSトラフィックを収集できる必要もあります。

このアドバイザリ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-20160302-openssl

該当製品

シスコでは現在、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、製品ラインを調査中です。このドキュメントでは、調査の進展に応じて、影響を受ける製品の Cisco Bug ID が更新されます。Cisco Bug ID は Cisco Bug Search Tool を使用してアクセス可能であり、回避策（使用可能な場合）と修正されたソフトウェア バージョンなど、プラットフォーム固有の追加情報が含まれます。

以下の製品については、本アドバイザリに記載された脆弱性の影響に関して現在調査中です。

調査中の製品

Unified Computing

- Cisco UCS Invicta Series Solid State Systems

シスコ ホステッド サービス

- Cisco UCS Invicta Series Autosupport Portal

脆弱性のある製品

次の表に、本アドバイザリに記載された 1 つ以上の脆弱性の影響を受けるシスコ製品を示します。

重要：次の表で、製品名の後にあるアスタリスク(*)は、DROWN攻撃に対して脆弱なシスコ製品を示しています。このドキュメントの発行時点で、25のシスコ製品がDROWN攻撃に対する脆弱性を持つことが判明しています。

製品	Cisco Bug ID	Fixed Release Availability
Collaboration and Social Media		
Cisco MeetingPlace	CSCuy54660	
Cisco SocialMiner	CSCuy74298	
Cisco WebEx Meetings Server versions 1.x	CSCuy54463	2.6.2 （2016年4月15日）
Cisco WebEx Meetings Server versions 2.x	CSCuy54463	2.6.2 （2016年4月15日）
Cisco WebEx Node for MCS	CSCuy54457	
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	CSCuy54595	
Cisco AnyConnect Secure Mobility Client for Android	CSCuy54599	
Cisco AnyConnect Secure Mobility Client for Android	CSCuy54600	
Cisco AnyConnect Secure Mobility Client for Linux	CSCuy54599	
Cisco AnyConnect Secure Mobility	CSCuy54599	

Client for OS X		
Cisco AnyConnect Secure Mobility Client for Windows	CSCuy54599	
Cisco AnyConnect Secure Mobility Client for iOS	CSCuy54599	
Cisco Jabber Guest 10.0(2)	CSCuy54659	
Cisco Jabber Software Development Kit	CSCuy54657	
Cisco Jabber for Android	CSCuy54676	
Cisco Jabber for Mac	CSCuy59818	11.6 （2016年3月23日） 11.7 （2016年3月23日）
Cisco Jabber for Windows	CSCuy62564	
Cisco MMP サーバ	CSCuy54470	
Cisco Webex Meetings Client - ホスト型	CSCuy54468	
Cisco WebEx Meetingsクライアント – オンプレミス	CSCuy54461	
Cisco WebEx Meetings for Android	CSCuy54458	
Cisco WebEx Meetings for WP8	CSCuy54460	
JCF コンポーネント	CSCuy56053	11.6 （2016年3月23日）
WebEx Meetings Server - SSL Gateway	CSCuy54464	2.6.2 （2016年4月15日）
WebEx Recording Playback Client	CSCuy54467	
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 ACE 30 Application Control Engine Module	CSCuy54474	
Cisco ACE 4710 Application Control Engine（A5）	CSCuy54474	
Cisco Application and Content Networking System(ACNS)(*)	CSCuy54560	5.5.41 （2016年4月15日）
Cisco InTracer	CSCuy54435	
Cisco Network Admission Control (NAC)	CSCuy54561	
Cisco Visual Quality Experience Server	CSCuy54558	
Cisco Visual Quality Experience	CSCuy54558	

Tools Server		
Cisco Wide Area Application Services（WAAS）	CSCuy58094	
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 CX と Cisco Prime Security Manager	CSCuy54575	9.3.4.5（2016年5月30日）
Cisco ASA Next-Generation Firewall Services	CSCuy54572	
Cisco Adaptive Security Appliance（ASA）	CSCuy54567	
Cisco Clean Access Manager	CSCuy54562	
Cisco Content Security Appliance Updater Servers	CSCuy54455	
Cisco Content Security Management Appliance (SMA)	CSCuy53668	
Cisco Email Security Appliance (ESA)	CSCuy53654	10.0（2016年6月下旬）
Cisco FireSIGHT システム ソフトウェア	CSCuy54453	
Cisco IPS(*)	CSCuy54601	7.1(11)パッチ2（2016年8月） 7.3(05)パッチ2（2016年11月）
Cisco Identity Services Engine（ISE）	CSCuy54586	
Cisco IronPort Encryption Appliance（IEA）	CSCuy54452	製品がEoLであるため、修正は予定されていません。
Cisco NAC Guest Server	CSCuy54564	
Cisco NAC Server	CSCuy54563	
Cisco Physical Access Control Gateway	CSCuy54579	
Cisco Secure Access Control Server（ACS）	CSCuy54597	
Cisco Virtual Security Gateway for Microsoft Hyper-V	CSCuy54498	
Cisco Web Security Appliance (WSA)	CSCuy54456	10.0（2016年6月下旬）
ネットワーク管理とプロビジョニング		
Cisco Application Networking	CSCuy54475	

Manager		
Cisco Application Policy Infrastructure Controller（APIC）	CSCuy54481	
Cisco Cloupia Unified Infrastructure Controller	CSCuy54478	該当するバージョンは5.5リリースでアップデートされます。
Cisco Digital Media Manager	CSCuy54532	5.3（2016年4月28日） 5.3.6（2016年4月28日） 5.3.6(RB1)（2016年4月28日） 5.3.6(RB2)（2016年4月28日） 5.4（2016年4月28日） 5.4.1（2016年4月28日） 5.4.1(RB1)（2016年4月28日） 5.4.1(RB2)（2016年4月28日）
Cisco MATE Collector	CSCuy58728	
Cisco MATE Design	CSCuy58728	
Cisco MATE Live	CSCuy58728	
Cisco管理アプライアンス(MAP)(*)	CSCuy54443	該当するシステムは2016年4月8日にアップデートされる予定です。
Cisco Mobile Wireless Transport Manager	CSCuy54523	
Cisco Multicast Manager	CSCuy54509	
Cisco NetFlow Generation Appliance	CSCuy54519	
Cisco Network Analysis Module	CSCuy54516	
Cisco Packet Tracer	CSCuy54539	7.0（2016年7月29日）
Cisco Policy Suite(CPS)	CSCuy58727	9.1（2016年4月30日）
Cisco Prime Access Registrar	CSCuy54512	7.1（2016年4月15日）
Cisco Prime Collaboration Assurance	CSCuy54522	
Cisco Prime Collaboration Deployment	CSCuy54636	
Cisco Prime Collaboration Provisioning	CSCuy54521	影響を受けるバージョンはすべて更新されています。
Cisco Prime Data Center Network Manager（DCNM）	CSCuy54479	10.0(1) (April 2016)
Cisco Prime Home	CSCuy54520	
Cisco Prime IP Express(*)	CSCuy54514	
Cisco Prime Infrastructure	CSCuy54517	

Standalone Plug and Play Gateway		
Cisco Prime Infrastructure	CSCuy54518	
Cisco Prime LAN Management Solution（LMS - Solaris）	CSCuy54508	
Cisco Prime License Manager	CSCuy54540	
Cisco Prime Network Registrar(CPNR)(*)	CSCuy54510	
Cisco Prime Network Services Controller(*)	CSCuy54525	3.4.2（2016年5月30日）
Cisco Prime Network	CSCuy54504	4.3 (July 2016)
Cisco Prime Optical for SPs	CSCuy54513	
Cisco Prime Performance Manager	CSCuy54505	1.7SP4（2016年4月27日）
Cisco Prime Security Manager	CSCuy54569	9.3.4.5（2016年5月30日）
Cisco Security Manager	CSCuy54524	
Cisco Show and Share（SnS）	CSCuy54542	
Cisco UCS Central	CSCuy54500	
Cisco Unified Intelligence Center（CUIC）	CSCuy74294	
Local Collector Appliance（LCA）	CSCuy54701	
StealthWatch FlowCollector NetFlow		
StealthWatch FlowCollector sFlow		
Stealthwatch Identity		
StealthWatch管理コンソール(SMC)		
StealthWatch UDP Director（以前の Flow Replicator）		
Routing and Switching - Enterprise and Service Provider		
Cisco 910 Industrial Router	CSCuy54697	IR910ではSSLv2が無効になっています。
Cisco ASR 5000 シリーズ	CSCuy54436	
Cisco Connected Gridルータ – CGOS (*)	CSCuy54477	16.2(00.192)（2016年4月7日）
Cisco Connected Grid ルータ	CSCuy54626	影響を受けるシステムはアップグレード済み。
Cisco IOS Software and Cisco IOS XE Software	CSCuy54623	

Cisco IOS XR ソフトウェア	CSCuy54527	
Cisco MDS 9000 Series Multilayer Switches	CSCuy54488	7.3.1.DX（2016年8月） 6.2.17 (June 2016) 7.3.1.NX（2016年8月） 7.0.3.I3（2016年5月） 8.3（2016年11月）
Cisco Nexus 1000V InterCloud(*)	CSCuy54485	1.0.1f（2016年3月21日） 1.0.1h4.4（2016年3月21日）
Cisco Nexus 1000V シリーズ スイッチ（ESX）	CSCuy54492	5.2(1)SV3(2.0.200)（2016年4月5日）
Cisco Nexus 3000 Series Switches	CSCuy54488	7.3.1.DX（2016年8月） 6.2.17 (June 2016) 7.3.1.NX（2016年8月） 7.0.3.I3（2016年5月） 8.3（2016年11月）
Cisco Nexus 4000 Series Blade Switches	CSCuy54603	4.1(2)E1(1q)（2016年6月30日）
Cisco Nexus 5000 Series Switches	CSCuy54488	7.3.1.DX（2016年8月） 6.2.17 (June 2016) 7.3.1.NX（2016年8月） 7.0.3.I3（2016年5月） 8.3（2016年11月）
Cisco Nexus 6000 Series Switches	CSCuy54488	7.3.1.DX（2016年8月） 6.2.17 (June 2016) 7.3.1.NX（2016年8月） 7.0.3.I3（2016年5月） 8.3（2016年11月）
Cisco Nexus 7000 Series Switches	CSCuy54488	7.3.1.DX（2016年8月） 6.2.17 (June 2016) 7.3.1.NX（2016年8月） 7.0.3.I3（2016年5月） 8.3（2016年11月）
Cisco Nexus 9000 (ACI/Fabric Switch)	CSCuy54484	2.0.1x（2016年6月）
Cisco Nexus 9000シリーズ（スタンドアロン、NX-OSを実行）	CSCuy57853	7.0(3)I4(1)（2016年3月25日） 7.0(3)I4(0.42)（2016年3月25日）
Cisco ONS 15454シリーズマルチサービスプロビジョニングプラットフォーム(*)	CSCuy54696	

Cisco OnePK All-in-One VM	CSCuy54577	
Cisco Service Control Operating System	CSCuy54627	
ルーティングおよびスイッチング - スモール ビジネス		
Cisco Sx220スイッチ	CSCuy54591	1.4.5.1 (May 2016)
Cisco Sx300スイッチ	CSCuy54592	1.4.5.1 (May 2016)
Cisco Sx500スイッチ	CSCuy54593	1.4.5.1 (May 2016)
Unified Computing		
Cisco Common Services Platform Collector	CSCuy54437	Affected systems have been updated.
Cisco Standalone ラック サーバ CIMC	CSCuy54501	
Cisco Unified Computing System (Management software)	CSCuy54576	
Cisco Unified Computing System Bシリーズ（ブレード）サーバ(*)	CSCuy54499	2.2(3d)以降は影響を受けません。Bシリーズサーバの場合は、このバージョン以降にアップグレードしてください。
Cisco Virtual Security Gateway	CSCuy54497	
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 190 ATA Series Analog Terminal Adaptor	CSCuy54633	
Cisco ATA 187 Analog Telephone Adaptor	CSCuy54665	
Cisco Agent Desktop for Cisco Unified Contact Center Express	CSCuy54639	
Cisco Agent Desktop	CSCuy54687	
Cisco Computer Telephony Integration Object Server（CTIOS）	CSCuy54688	
Cisco Emergency Responder	CSCuy54646	
Cisco Finesse	CSCuy54645	
Cisco Hosted Collaboration Mediation Fulfillment	CSCuy54652	
Cisco IM and Presence Service（CUPS）	CSCuy54649	
Cisco IP Interoperability and	CSCuy54549	

Collaboration System (IPICS)		
Cisco Jabber for iOS	CSCuy54655	
Cisco MediaSense	CSCuy54668	
Cisco Packaged Contact Center Enterprise	CSCuy54689	
Cisco Paging Server（Informacast）	CSCuy54654	
Cisco Paging Server	CSCuy54654	
Cisco SPA112 2-Port Phone Adapter	CSCuy54587	
Cisco SPA122 ATA with Router	CSCuy54587	
Cisco SPA232D Multi-Line DECT ATA	CSCuy54587	
Cisco SPA30X Series IP Phones	CSCuy54590	
Cisco SPA50X Series IP Phones	CSCuy54590	
Cisco SPA51X Series IP Phones	CSCuy54590	
Cisco SPA525G	CSCuy54588	
Cisco TAPI Service Provider（TSP）	CSCuy54635	
Cisco Unified 6901 IP フォン	CSCuy54661	
Cisco Unified 6945 IP フォン	CSCuy54666	
Cisco Unified 7800 Series IP Phones	CSCuy54672	
Cisco Unified 8831 シリーズ IP Conference Phone	CSCuy54663	
Cisco Unified 8945 IP フォン	CSCuy54662	
Cisco Unified 8961 IP フォン	CSCuy54651	
Cisco Unified 9951 IP フォン	CSCuy54651	
Cisco Unified 9971 IP フォン	CSCuy54651	
Cisco Unified Attendant Console Advanced	CSCuy54630	
Cisco Unified Attendant Console Business Edition	CSCuy54630	
Cisco Unified Attendant Console Department Edition	CSCuy54630	
Cisco Unified Attendant Console Enterprise Edition	CSCuy54630	
Cisco Unified Attendant Console	CSCuy54630	

Premium Edition		
Cisco Unified Attendant Console Standard	CSCuy54631	
Cisco Unified Communications Domain Manager	CSCuy54640	11.5.1（2016年8月）
Cisco Unified Communications Manager（UCM）	CSCuy54634	
Cisco Unified Communications Manager Session Management Edition（SME）	CSCuy54634	
Cisco Unified Communications for Microsoft Lync	CSCuy54641	
Cisco Unified Contact Center Enterprise	CSCuy54688	
Cisco Unified Contact Center Express	CSCuy74300	
Cisco Unified IP Conference Phone 8831 for Third-Party Call Control	CSCuy54629	
Cisco Unified IP Phone 7900 Series	CSCuy54674	
Cisco Unified Intelligent Contact Management Enterprise	CSCuy54688	
Cisco Unified Wireless IP Phone	CSCuy54681	SSLv2は無効です。
Cisco Unified Workforce Optimization	CSCuy54680	WFO 10.5（2016年3月31日） WFO 11.0（2016年4月15日）
Cisco Unity Connection（UC）	CSCuy54637	
Cisco Virtualization Experience Media Engine	CSCuy54679	11.7（2016年7月28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 AnyRes Live（CAL）	CSCuy54616	9.6.4 (April 2016)
Cisco DCM Series 9900-Digital Content Manager	CSCuy54502	
Cisco Digital Media Players (DMP) 4300 Series	CSCuy54531	5.4(1)（2016年4月10日）
Cisco Digital Media Players (DMP) 4400 Series	CSCuy54531	5.4(1)（2016年4月10日）
Cisco Edge 300 Digital Media Player	CSCuy54698	1.6RB4_4（2016年4月15日）
Cisco Edge 340 Digital Media Player	CSCuy54700	該当するシステムは、2016年4月15日

		までにアップデートされる予定です。
Cisco Enterprise Content Delivery System (ECDS)	CSCuy54533	2.6.7 （ 2016年4月15日 ）
Cisco Expressway シリーズ(*)	CSCuy54547	
シスコヘッドエンドシステムリリース(*)	CSCuy54611	1.06 （ 2016年5月1日 ） 1.1.3 （ 2016年5月1日 ） 2.0.10 （ 2016年5月1日 ） 2.1.2 （ 2016年5月1日 ） 3.0.4 （ 2016年5月1日 ）
Cisco Media Experience Engines(MXE)(*)	CSCuy54538	
Cisco Media Services Interface	CSCuy54528	
Cisco Model D9485 DAVIC QPSK (*)	CSCuy54612	1.2.4 （ 2016年8月31日 ）
Cisco TelePresence 1310(*)	CSCuy54628	
Cisco TelePresence Conductor	CSCuy54529	SSLv2は、ソフトウェアバージョンXC4.0以降では無効になっています。
Cisco TelePresence Content Server （ TCS ）	CSCuy54545	
Cisco TelePresence ISDN GW 3241	CSCuy54534	
Cisco TelePresence ISDN GW MSE 8321	CSCuy54534	
Cisco TelePresence ISDN Link	CSCuy54535	
Cisco TelePresence MCU (8510, 8420, 4200, 4500 and 5300)	CSCuy54536	
Cisco TelePresence Serial Gateway Series	CSCuy54541	
Cisco TelePresence Server 8710、7010	CSCuy54546	
Cisco TelePresence Server on Multiparty Media 310、320	CSCuy54546	
Cisco TelePresence Server on Virtual Machine	CSCuy54546	
Cisco TelePresence Supervisor MSE 8050	CSCuy54537	
Cisco TelePresenceシステム1000(*)	CSCuy54628	
Cisco TelePresenceシステム1100(*)	CSCuy54628	

Cisco TelePresenceシステム1300(*)	CSCuy54628	
Cisco TelePresence System 3000シリーズ(*)	CSCuy54628	
Cisco TelePresenceシステム500-32(*)	CSCuy54628	
Cisco TelePresenceシステム500-37(*)	CSCuy54628	
Cisco TelePresence TX 9000シリーズ(*)	CSCuy54628	
Cisco TelePresence Video Communication Server(VCS)(*)	CSCuy54547	
Cisco VEN501 Wireless Access Point	CSCuy54550	
Cisco Video Distribution Suite for Internet Streaming（VDS-IS/CDS-IS）	CSCuy54553	4.3.2 (May 2016)
Cisco Video Surveillance 3000 Series IP Cameras	CSCuy54583	
Cisco Video Surveillance 3000 Series IP Cameras	CSCuy54584	SSLv2はサポートされていません。
Cisco Video Surveillance 4000 Series High-Definition IP Cameras	CSCuy54580	
Cisco Video Surveillance 4300E/4500E High-Definition IP Cameras	CSCuy54581	
Cisco Video Surveillance 6000 Series IP Cameras	CSCuy54583	
Cisco Video Surveillance 6000 Series IP Cameras	CSCuy54584	SSLv2はサポートされていません。
Cisco Video Surveillance 7000 Series IP Cameras	CSCuy54583	
Cisco Video Surveillance 7000 Series IP Cameras	CSCuy54584	SSLv2はサポートされていません。
Cisco Video Surveillance Media Server	CSCuy54585	7.8（2016年7月1日）
Cisco Video Surveillance PTZ IP Cameras	CSCuy54583	

Cisco Video Surveillance PTZ IP Cameras	CSCuy54584	SSLv2はサポートされていません。
Cisco Videoscape Control Suite	CSCuy54551	3.6.0（2016年4月30日）
クラウドオブジェクトストア(COS)(*)	CSCuy54552	3.8.0（2016年3月30日）
Tandberg Codian ISDN GW 3210/3220/3240	CSCuy54534	
Tandberg Codian MSE 8320 model	CSCuy54534	
ワイヤレス		
Cisco Aironet 2700 シリーズ アクセス ポイント	CSCuy54506	
Cisco Mobility Services Engine（MSE）	CSCuy58090	
Ciscoワイヤレス LANコントローラ(WLC)(*)	CSCuy58091	8.0 (April 2016) 8.3 (May 2016)
シスコ ホステッド サービス		
Cisco Intelligent Automation for Cloud	CSCuy54548	
Cisco Proactive Network Operations Center	CSCuy54441	
Cisco Registered Envelope Service（CRES）	CSCuy54451	
Cisco Services Provisioning Platform（SPP）	CSCuy54682	
Cisco Smart Care	CSCuy54565	
Cisco Universal Small Cell 5000 シリーズ（V3.4.2.x ソフトウェアを実行）	CSCuy54610	
Cisco Universal Small Cell 7000 シリーズ（V3.4.2.x ソフトウェアを実行）	CSCuy54610	
Cisco Universal Small Cell usc-iuh	CSCuy54608	
Cisco WebEx Connect クライアント（Windows）	CSCuy54465	
Cisco WebEx Meeting Center	CSCuy54473	
Cisco WebEx Meetings (Meeting Center, Training Center, Event	CSCuy54472	

Center, Support Center)		
Cisco WebEx Messenger Service	CSCuy54466	
Network Health Framework (NHF)	CSCuy54702	
Network Performance Analytics (NPA)	CSCuy54703	
Partner Supporting Service（PSS）1.x	CSCuy54568	
Serial Number Assessment Service（SNAS）	CSCuy54571	
Services Analytic Platform	CSCuy54445	
Small Cell factory recovery root filesystem V2.99.4 or later	CSCuy54607	

脆弱性を含んでいないことが確認された製品

シスコは、本アドバイザリに記載された脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

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 WebEx Meetings for BlackBerry
- Cisco WebEx Productivity Tools

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 Content Security and Control（CSC）Security Services Module

ネットワーク管理とプロビジョニング

- Cisco Configuration Professional
- Cisco Prime LAN Management Solution（LMS:WindowsおよびLinux）
- Cisco Prime Network Registrar IP アドレス マネージャ（IPAM）

Routing and Switching - Enterprise and Service Provider

- Cisco Broadband Access Center Telco Wireless
- Cisco IOS XE（SSL VPN 機能）

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 7937 IP Phone
- Cisco 8800 Series IP Phones - VPN Feature
- Cisco DX シリーズ IP フォン
- Cisco Remote Silent Monitoring
- 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 Unified E-Mail Interaction Manager
- Cisco Unified Sip Proxy
- Cisco Unified Web Interaction Manager
- Cisco Virtual PGW 2200 ソフトスイッチ
- Cisco Voice Portal（CVP）

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 AnyRes VOD（CAL）
- Cisco D9859 Advanced Receiver Transcoder
- Cisco TelePresence EX Series
- Cisco TelePresence MX Series
- Cisco TelePresence Profile Series
- Cisco TelePresence SX Series
- Cisco TelePresence Integrator C Series

シスコ ホステッド サービス

- Cisco Cloud Web Security
- Cisco Connected Analytics For Collaboration
- Cisco One Portal
- Cisco SmartConnection
- Cisco SmartReports
- Cisco Unified Services Delivery Platform（CUSDP）
- コミュニケーション/コラボレーションサイジングツール、仮想マシン配置ツール、Cisco Unified Communications Upgrade Readiness Assessment
- Life Cycle Management Agent Manager（LCM）

詳細

2016年3月1日にOpenSSL Software Foundationのセキュリティアドバイザリで公開された脆弱性の名前とそれに関連するCommon Vulnerabilities and Exposures(CVE)IDは次のとおりです。

複数ベンダーのSSL/TLS実装におけるDROWN情報漏えいの脆弱性

SSL/TLSを使用する複数ベンダー製品の脆弱性により、認証されていないリモートの攻撃者がObsolete and Wearded eCryption(DROWN)クロスプロトコル攻撃を使用して復号化RSAを実行し、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、Transport Layer Security(TLS)内で脆弱なRivest, Shamir, and Adleman(RSA)暗号スイートの使用を可能にする可能性があるSSLv2プロトコルの実装エラーに起因します。 攻撃者は、ターゲットシステムと、同じ秘密キーを使用して接続の1つを監視し、場合によっては復号化する脆弱なSSLv2サーバの間のトラフィックを傍受することで、この脆弱性を不正利用する可能性があります。攻撃者は、復号化された暗号文をターゲットサーバに返し、サーバの応答から判断して、暗号化された通信で使用される秘密鍵を判別する可能性があります。この不正利用により、攻撃者は標的となるクライアントとSSLv2サーバ間のTLSセッションを復号化し、機密情報へのアクセスに利用する可能性があります。

本脆弱性のIDは、CVE ID CVE-2016-0800です。

OpenSSL Bleichenbacher保護セキュリティバイパスの脆弱性

OpenSSLのSSLv2プロトコル実装における脆弱性により、認証されていないリモートの攻撃者がセキュリティ制限をバイパスできる可能性があります。

この脆弱性は、該当ソフトウェアによるエクスポート暗号スイートに対するBleichenbacher保護の不適切な実装に起因します。攻撃者は、この脆弱性を不正利用してBleichenbacher oracleを確立し、Decrypting RSA with Obsolete and Weaked eEncryption(DROWN)攻撃の多様な実行を支援する可能性があります。

本脆弱性のIDは、CVE ID CVE-2016-0704です。

OpenSSL SSLv2のマスターキー回復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、影響を受けるソフトウェアによって実装されたセキュリティ制限が不適切なことに起因します。認証されていないリモートの攻撃者が、通信トラフィックを傍受することで、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。

本脆弱性のIDは、CVE ID CVE-2016-0703です。

OpenSSLデジタル署名アルゴリズムの秘密鍵の処理における二重解放の脆弱性

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、該当ソフトウェアによる不正なデジタル署名アルゴリズム(DSA)秘密キーの不適切な解析に起因します。攻撃者は、不正な形式のDSA秘密キーをアプリケーションと交換しようとする攻撃者が制御するサーバに接続するために、脆弱なバージョンのOpenSSLを使用するアプリケーションのユーザを誘導することで、この脆弱性をエクスプロイトする可能性があります。この不正利用により、メモリの二重空き状態が引き起こされ、攻撃者はこれを利用してDoS状態を引き起こす可能性があります。

本脆弱性のIDは、CVE ID CVE-2016-0705です。

OpenSSL SRP_VBASE_get_by_userメソッドのメモリリークの脆弱性

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、不適切なメモリ処理に起因します。認証されていないリモートの攻撃者が、悪意のあるログイン要求をSRPユーザデータベースに送信することで、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、攻撃者は該当システムでメモリリークを引き起こし、その結果DoS状態が発生する可能性があります。

本脆弱性のIDは、CVE ID CVE-2016-0798です。

OpenSSL BN_hex2bnおよびBN_dec2bn関数NULLポインタ逆参照の脆弱性

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不適切なメモリ操作が実行されることに起因します。認証されていないリモートの攻撃者は、巧妙に細工された入力を送信して該当ソフトウェアで処理することにより、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はアプリケーションを断続的に停止させ、DoS状態を引き起こす可能性があります。

本脆弱性のIDは、CVE ID CVE-2016-0797です。

OpenSSL BIO_*printf関数の範囲外のメモリ読み取りの脆弱性

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、影響を受けるソフトウェアによって実行される境界チェックが不適切なことに起

因します。認証されていないリモートの攻撃者は、巧妙に細工された入力を送信して該当ソフトウェアで処理することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は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。

本脆弱性のIDは、CVE-2016-0799およびCVE-2016-2842です。

OpenSSL RSA暗号化キー回復の脆弱性

OpenSSLの脆弱性により、認証されていないローカル攻撃者が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、該当ソフトウェアによる不適切なメモリ管理に起因します。認証されていないローカルの攻撃者が、該当ソフトウェアに悪意のあるコードを注入することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は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。

本脆弱性のIDは、CVE ID CVE-2016-0702です。

回避策

回避策は今後 Cisco bugs に記載され、Cisco Bug Search Tool を使用して検索可能です。

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、シスコから直接、あるいはシスコ認定リセラーまたはパートナーからそのソフトウェアの有効なライセンスを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。

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を確認していません。

出典

これらの脆弱性は、2016年3月1日に OpenSSL Software Foundationによって公開されました。

このDROWN攻撃は、Nimrod Aviram、Sebastian Schinzel、Juraj Somorovsky、Nadia Heninger、Maik Dankel、Jens Steube、Luke Valenta、Shaanan Cohney、Susanne Engels、Christof Paar、およびYuval ShavittによってCisco PSIRTに個別に報告されました。シスコは、攻撃を報告していただき、攻撃の開示に関して調整を行っていただいたことに対して、お礼を申し上げます。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-openssl

改訂履歴

バージョン	説明	セクション	ステータス	日付
2.2	脆弱性のある製品のリストを更新。	「該当製品」、「脆弱性のある製品」	Interim	2016年5月23日
2.1	調査中の製品、脆弱性のある製品、脆弱性を含んでいない製品のリストを更新。	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	2016年5月11日
2.0	調査中の製品、脆弱性のある製品、脆弱性を含んでいない製品のリストを更新。	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	2016年5月2日
1.9	調査中または脆弱性のある製品のリストを更新。	「該当製品」、「脆弱性のある製品」	Interim	2016年4月11日
1.8	調査中の製品、脆弱性のある製品、脆弱性を含んでいない製品のリストを更新。	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	2016年4月1日
1.7	調査中の製品、脆弱性のある製品、脆弱性を含んでいない製品のリストを更新。	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	2016年3月18日
1.6	調査中の製品、脆弱性のある製品、脆弱性を含んでいない製品のリストを更新。	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	2016年3月15日
1.5	調査中の製品、脆弱性のある製品、脆弱性を含んでいない製品のリストを更新。	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	2016年3月10日
1.4	調査中の製品、脆弱性のある製品、脆弱性を含んでいない製品のリストを更新。	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	2016年3月9日
1.3	調査中の製品、脆弱性のある製品、脆弱性を含んでいない製品のリストを更新。	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	2016年3月8日
1.2	調査中の製品、脆弱性のある製品、脆弱性を含んでいない製品のリストを更新。	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	2016年3月4日
1.1	調査中の製品、脆弱性のある製品、脆弱性を含んでいない製品のリストを更新。	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	2016 年 3 月 3 日

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Interim	2016 年 3 月 2 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。