

シスコ製品に影響するOpenSSLの複数の脆弱性 : 2016年5月



アドバイザーID : [cisco-sa-20160504-openssl](#) [CVE-2016-2106](#)
初公開日 : 2016-05-04 19:30 [CVE-2016-2107](#)
最終更新日 : 2016-12-05 16:10 [CVE-2016-2108](#)
バージョン 1.12 : Final [CVE-2016-2109](#)
回避策 : No workarounds available [CVE-2016-2105](#)
Cisco バグ ID : [CSCuz52522](#) [CSCuz52407](#) [CVE-2016-2176](#)
[CSCuz52528](#) [CSCuz52408](#) [CSCuz52529](#)
[CSCuz52405](#) [CSCuz52409](#) [CSCuz52490](#)
[CSCuz52370](#) [CSCuz63935](#) [CSCuz63936](#)
[CSCuz52373](#) [CSCuz52494](#) [CSCuz63938](#)
[CSCuz52371](#) [CSCuz52492](#) [CSCuz52493](#)
[CSCuz52410](#) [CSCuz52531](#) [CSCuz52532](#)
[CSCuz52375](#) [CSCuz52415](#) [CSCuz52533](#)
[CSCuz52413](#) [CSCuz52418](#) [CSCuz52539](#)
[CSCuz52537](#) [CSCuz52538](#) [CSCuz63940](#)
[CSCuz52382](#) [CSCuz52383](#) [CSCuz52421](#)
[CSCuz52422](#) [CSCuz52543](#) [CSCuz52386](#)
[CSCuz52387](#) [CSCuz52420](#) [CSCuz52348](#)
[CSCuz52349](#) [CSCuz52503](#) [CSCuz52468](#)
[CSCuz52506](#) [CSCuz52507](#) [CSCuz52508](#)
[CSCuz52351](#) [CSCuz52472](#) [CSCuz52477](#)
[CSCuz52474](#) [CSCuz55590](#) [CSCuz52362](#)
[CSCuz52483](#) [CSCuz52363](#) [CSCuz52360](#)
[CSCuz52481](#) [CSCuz52482](#) [CSCuz52366](#)
[CSCuz52487](#) [CSCuz52367](#) [CSCuz52400](#)
[CSCuz52488](#) [CSCuz52364](#) [CSCuz52485](#)
[CSCuz73565](#) [CSCuz52365](#) [CSCuz52486](#)
[CSCuz52447](#) [CSCuz52568](#) [CSCuz52448](#)
[CSCuz52566](#) [CSCuz52446](#) [CSCuz52567](#)
[CSCuz52571](#) [CSCuz52451](#) [CSCuz52570](#)
[CSCuz52454](#) [CSCuz52455](#) [CSCuz52452](#)
[CSCuz52453](#) [CSCuz52458](#) [CSCuz52456](#)
[CSCuz52461](#) [CSCuz52462](#) [CSCuz52583](#)
[CSCuz52466](#) [CSCuz52587](#) [CSCuz52425](#)
[CSCuz52547](#) [CSCuz52423](#) [CSCuz52424](#)
[CSCuz52429](#) [CSCuz52548](#) [CSCuz60563](#)

[CSCuz52550](#) [CSCuz52393](#) [CSCuz52399](#)
[CSCuz52432](#) [CSCuz52433](#) [CSCuz52554](#)
[CSCuz52397](#) [CSCuz52430](#) [CSCuz52551](#)
[CSCuz52552](#) [CSCuz52437](#) [CSCuz52558](#)
[CSCuz52435](#) [CSCuz52556](#) [CSCuz52439](#)
[CSCuz52560](#) [CSCuz52444](#) [CSCuz52565](#)
[CSCuz52441](#) [CSCuz52562](#) [CSCuz52442](#)
[CSCuz52563](#)

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5月3日、OpenSSL Software Foundationから6件の脆弱性を含むセキュリティアドバイザリがリリースされました。公開されている6つの脆弱性のうち、4つはメモリの破損または過剰なメモリ使用を引き起こす可能性があり、接続でAES CBC暗号が使用され、サーバがAES-NIをサポートしている場合は、padding oracle攻撃によってトラフィックを復号化できる可能性があります。最後に、Extended Binary Coded Decimal Interchange Code(EBCDIC)符号化を使用して操作をする製品に固有です。

複数のシスコ製品に、1つ以上の脆弱性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。

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-20160504-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。製品が該当するかどうかについては、このアドバイザリの「脆弱性が存在する製品」および「脆弱性を含まないことが確認された製品」のセクションを参照してください。

「脆弱性が存在する製品」セクションに、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。

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。

製品	Cisco Bug ID	Fixed Release Availability
Collaboration and Social Media		
Cisco MeetingPlace	0.CSCuz52556	CWMS 2.7 (入手可能)
Cisco SocialMiner	0.CSCuz63938	11.5.1 (入手可能)
Cisco WebEx Meetings Server versions 1.x	0.CSCuz52375	" 2.6.1.2109 (入手可能) 2.7.1.12 (入手可能)
Cisco WebEx Meetings Server versions 2.x	0.CSCuz52375	" 2.6.1.2109 (入手可能) 2.7.1.12 (入手可能)
Cisco WebEx Node for MCS	0.CSCuz52370	3.12.9.8 (入手可能)
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	0.CSCuz52503	2.1.5(N3K/N9K) (入手可能) 2.0.7(N7K) (入手可能) 2.0.7(cat3k/cat4k) (入手可能)
Cisco AnyConnect Secure Mobility Client for Android	0.CSCuz52506	4.3 for Windows Linux OS X (2016年6月10日) 4.2 for Windows Linux OS X (2016年6月16日) 4.0 for Android iOS (2016年6月30日)
Cisco AnyConnect Secure Mobility Client for Android	0.CSCuz52507	4.3 for Windows Linux OS X (入手可能) 4.2 for Windows Linux Android向けOS X (入手可能) 4.0 iOS (使用可能)
Cisco AnyConnect Secure Mobility Client for Linux	0.CSCuz52506	4.3 for Windows Linux OS X (2016年6月10日) 4.2 for Windows Linux OS X (2016年6月16日) 4.0 for Android iOS (2016年6月30日)

Cisco AnyConnect Secure Mobility Client for OS X	0.CSCuz52506	4.3 for Windows Linux OS X (2016年6月10日) 4.2 for Windows Linux OS X (2016年6月16日) 4.0 for Android iOS (2016年6月30日)
Cisco AnyConnect Secure Mobility Client for Windows	0.CSCuz52506	4.3 for Windows Linux OS X (2016年6月10日) 4.2 for Windows Linux OS X (2016年6月16日) 4.0 for Android iOS (2016年6月30日)
Cisco AnyConnect Secure Mobility Client for iOS	0.CSCuz52506	4.3 for Windows Linux OS X (2016年6月10日) 4.2 for Windows Linux OS X (2016年6月16日) 4.0 for Android iOS (2016年6月30日)
Cisco Jabber Guest 10.0(2)	0.CSCuz52554	11.0 (Available)
Cisco Jabber Software Development Kit	0.CSCuz52552	11.7 (Available)
Cisco Jabber for Android	0.CSCuz52568	11.6 MR (入手可能)
Cisco Jabber for Mac	0.CSCuz52551	11.7 (Available)
Cisco Jabber for Windows	0.CSCuz60563	11.6(1) (入手可能)
Cisco MMP サーバ	0.CSCuz52380	3.10.0 (入手可能)
Cisco Webex Meetings Client - ホスト型	0.CSCuz52379	T31R1SP6 (2016年12月15日)
Cisco WebEx Meetings Client - On Premises	0.CSCuz52374	2.7.1.12 (入手可能) 2.6.1.2109 (入手可能)
Cisco WebEx Meetings for Android	0.CSCuz52371	脆弱性のあるリリースに対してパッチファイルを使用できます
Cisco WebEx Meetings for WP8	0.CSCuz52373	No further releases are planned
WebEx Meetings Server - SSL	0.CSCuz52376	"

Gateway		2.6.1.2109 (入手可能) 2.7.1.12 (入手可能)
WebEx Recording Playback Client	0.CSCuz52378	T31R1SP6 (2016年12月)
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	0.CSCuz52383	公開済みの修正プログラムはありません
Cisco ACE 4710 Application Control Engine (A5)	0.CSCuz52383	公開済みの修正プログラムはありません
Cisco Application and Content Networking System (ACNS)	0.CSCuz52468	5.5.41 (2016年7月31日)
Cisco InTracer	0.CSCuz52350	製品はEOLのため、修正は予定されていません。
Cisco Network Admission Control (NAC)	0.CSCuz52469	公開済みの修正プログラムはありません
Cisco Visual Quality Experience Server	0.CSCuz52466	3.11(3.1) (入手可能)
Cisco Visual Quality Experience Tools Server	0.CSCuz52466	3.11(3.1) (入手可能)
Cisco Wide Area Application Services (WAAS)	0.CSCuz52481	5.5.7 (2016年6月30日) 6.2.3 (2016年7月29日)
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	0.CSCuz52482	9.5.4.3 (2016年5月30日)
Cisco ASA Next-Generation Firewall Services	0.CSCuz52479	R2.1.1 (入手可能)
Cisco Adaptive Security Appliance (ASA)	0.CSCuz52474	影響を受けるすべてのシステムがアップデートされました。
Cisco Clean Access Manager	0.CSCuz52470	公開済みの修正プログラムはありません
Cisco Content Security Management Appliance (SMA)	0.CSCuz52367	10.5 (2017年4月)
Cisco FireSIGHT システム ソフトウェア	0.CSCuz52366	6.0.1.2 (2016年6月27日)
Cisco IPS	0.CSCuz52508	公開済みの修正プログラムはありません
Cisco Identity Services Engine (ISE)	0.CSCuz52493	2.2.1 (入手可能)

Cisco Email Security Appliance (ESA)	0.CSCuz52363	11.0 (2017年4月)
Cisco IronPort Encryption Appliance (IEA)	0.CSCuz52365	公開済みの修正プログラムはありません
Cisco NAC Guest Server	0.CSCuz52472	公開済みの修正プログラムはありません
Cisco NAC Server	0.CSCuz52471	公開済みの修正プログラムはありません
Cisco Physical Access Control Gateway	0.CSCuz52487	
Cisco Secure Access Control Server (ACS)	0.CSCuz52504	5.8パッチ5 (2016年7月)
Cisco Secure Access Control System (ACS)	0.CSCuz52505	5.8パッチ5 (入手可能)
Cisco Virtual Security Gateway for Microsoft Hyper-V	0.CSCuz52403	5.2(1) (2016年8月20日) VSG2(1.4) (2016年8月20日)
Cisco Web Security Appliance (WSA)	0.CSCuz52369	10.5 (2017年3月)
Lancope Stealthwatch SMC		6.7.3 2016年5月末 6.8.0 2016年5月末 6.8.1 2016年6月 6.8.2 2016年6月末
Lancope Stealthwatch FlowCollector NetFlow		6.7.3 2016年5月末 6.8.0 2016年5月末 6.8.1 2016年6月 6.8.2 2016年6月末
Lancope Stealthwatch FlowCollector sFlow		6.7.3 2016年5月末 6.8.0 2016年5月末 6.8.1 2016年6月 6.8.2 2016年6月末
Lancope Stealthwatch FlowSensor		6.7.3 2016年5月末 6.8.0 2016年5月末 6.8.1 2016年6月 6.8.2 2016年6月末
Lancope Stealthwatch UDP Director		6.7.3 2016年5月末 6.8.0 2016年5月末 6.8.1 2016年6月 6.8.2 2016年6月末

ネットワーク管理とプロビジョニング		
Cisco Application Networking Manager	0.CSCuz52384	アップグレードオプションについてはTACにお問い合わせください。
Cisco Application Policy Infrastructure Controller (APIC)	0.CSCuz52389	11.6 MR (入手可能)
Cisco Digital Media Manager	0.CSCuz52441	5.3.0 (入手可能) 5.3.6 (入手可能) 5.3.6(RB1) (入手可能) 5.3.6(RB2) (入手可能) 5.4.0 (入手可能) 5.4.1 (入手可能) 5.4.1(RB1) (入手可能) 5.4.1(RB2) (入手可能)
Cisco MATE Collector	0.CSCuz52583	6.3.5dev-19-g2329292 (入手可能) 6.4dev-2206-g9361bc4 (入手可能) 6.4dev-2250-g50ed411 (入手可能)
Cisco MATE Design	0.CSCuz52583	6.3.5dev-19-g2329292 (入手可能) 6.4dev-2206-g9361bc4 (入手可能) 6.4dev-2250-g50ed411 (入手可能)
Cisco MATE Live	0.CSCuz52583	6.3.5dev-19-g2329292 (入手可能) 6.4dev-2206-g9361bc4 (入手可能) 6.4dev-2250-g50ed411 (入手可能)
Cisco Management Appliance (MAP)	0.CSCuz52355	0.9.8e (入手可能) 0.9.8-39.el5_11 (2016年6月8日)
Cisco Mobile Wireless Transport Manager	0.CSCuz52431	修正予定なし.
Cisco NetFlow Generation Appliance	0.CSCuz52426	影響を受けるシステムは更新されます (2016年8月1日)
Cisco Network Analysis Module	0.CSCuz52423	6.3.1 (入手可能)
Cisco Packet Tracer	0.CSCuz52451	7.0 (Available)
Cisco Policy Suite(CPS)	0.CSCuz52587	10.0 (Available)
Cisco Prime Access Registrar	0.CSCuz52418	7.0.1.7 (2016年6月) 7.1.x (2016年6月) 7.2 (2016年9月)
Cisco Prime Collaboration Assurance	0.CSCuz52430	11.5 SP1 (2016年8月)
Cisco Prime Collaboration Deployment	0.CSCuz52537	11.5 (Available)

Cisco Prime Collaboration Provisioning	0.CSCuz52429	11.2 (Available)
Cisco Prime Data Center Network Manager (DCNM)	0.CSCuz52387	10.0(1.28)S0 (入手可能)
Cisco Prime IP Express	0.CSCuz52421	
Cisco Prime Infrastructure Standalone Plug and Play Gateway	0.CSCuz52424	
Cisco Prime Infrastructure	0.CSCuz52425	3.1.1 (2016年6月)
Cisco Prime LAN Management Solution (LMS - Solaris)	0.CSCuz52413	修正は必要ありません。
Cisco Prime License Manager	0.CSCuz52452	11.5 (2016年6月)
Cisco Prime Network Registrar (CPNR)	0.CSCuz52415	
Cisco Prime Network Services Controller	0.CSCuz52433	3.4.2 (AUG-2016)
Cisco Prime Network	0.CSCuz52408	影響を受けるシステムは更新されます (2016年6月30日)。
Cisco Prime Optical for SPs	0.CSCuz52420	10.6 (Available)
Cisco Prime Performance Manager	0.CSCuz52409	1.7.0.6 (2016年7月30日)
Cisco Prime Security Manager	0.CSCuz52477	9.5.4.3 (入手可能)
Cisco Security Manager	0.CSCuz52432	4.12 (Available)
Cisco UCS Central	0.CSCuz52405	1.5(1a) (入手可能)
Cisco Unified Intelligence Center (CUIC)	0.CSCuz63935	11.5.1 (入手可能)
Local Collector Appliance (LCA)	0.CSCuz52524	2.2.12 (2016年5月20日)
Routing and Switching - Enterprise and Service Provider		
Cisco ASR 5000 シリーズ	0.CSCuz52351	19.4.0 (2016年6月30日) 20.2.0 (2016年7月29日) 21.0.0 (2016年9月30日)
Cisco Connected Grid Router - CGOS	0.CSCuz52385	15.6.2.15T (2016年6月5日)
Cisco Connected Grid ルータ	0.CSCuz52529	15.6.2.15T (2016年6月5日)
Cisco IOS ソフトウェアと Cisco IOS-XE ソフトウェア	0.CSCuz52528	" 15.4(1)IA1.73 (入手可能) 15.6(2)T0.1 (入手可能)

		15.6(2.19)T (入手可能) 16.3(0.232) (入手可能) 16.4(0.49) (入手可能)
Cisco IOS-XR	0.CSCuz52437	影響を受けるシステムは更新されます (2016年6月8日)
Cisco MDS 9000 Series Multilayer Switches	0.CSCuz52394	6.2.17(MDS) (2016年6月) 7.3.1DX (N7kおよびMDS) (2016年8月) 7.3.1NX(N5k/N6k) (2016年8月) 8.3(N3k/N9k) (2016年11月)
Cisco Nexus 1000V InterCloud	0.CSCuz52393	影響を受けるシステムは更新されます (2016年6月30日)。
Cisco Nexus 1000V シリーズ スイッチ (ESX)	0.CSCuz52399	5.2(1)SV3(2.1) (2016年6月30日)
Cisco Nexus 1000V シリーズ スイッチ	0.CSCuz52397	5.2(1)SV3(2.1) (入手可能)
Cisco Nexus 3X00 シリーズ スイッチ	0.CSCuz52400	6.0(2)A8(1) (入手可能)
Cisco Nexus 4000 Series Blade Switches	0.CSCuz52512	0.9.8zf (入手可能)
Cisco Nexus 5000 Series Switches	0.CSCuz52401	7.3.1 (入手可能)
Cisco Nexus 6000 Series Switches	0.CSCuz52395	6.2.17(MDS) (2016年6月) 7.3.1DX (N7kおよびMDS) (2016年8月) 7.3.1NX(N5k/N6k) (2016年8月) 8.3(N3k/N9k) (2016年11月)
Cisco Nexus 7000 Series Switches	0.CSCuz52395	6.2.17(MDS) (2016年6月) 7.3.1DX (N7kおよびMDS) (2016年8月) 7.3.1NX(N5k/N6k) (2016年8月) 8.3(N3k/N9k) (2016年11月)
Cisco Nexus 9000 (ACI/Fabric Switch)	0.CSCuz52391	12.0(0.133) (入手可能)
Cisco Nexus 9000 シリーズ (スタンドアロン、NxOS を実行)	0.CSCuz52396	10.6(3.11002.7)
Cisco ONS 15454 Series Multiservice Provisioning Platforms	0.CSCuz52486	10.6.1 (2016年6月30日)
Cisco OnePK All-in-One VM	0.CSCuz52485	公開済みの修正プログラムはありません

		ん
Cisco Service Control Operating System	0.CSCuz52530	5.1 (Available) 5.2 (Available)
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 switches	0.CSCuz52497	1.4.7 (2016年11月)
Cisco Sx300 switches	0.CSCuz52500	1.4.7 (2016年11月)
Cisco Sx500 switches	0.CSCuz52502	1.4.7 (2016年11月)
Unified Computing		
Cisco Cloupia Unified Infrastructure Controller	0.CSCuz52386	5.5 (Available)
Cisco Common Services Platform Collector	0.CSCuz52352	1.10 (2016年9月)
Cisco Standalone ラック サーバ CIMC	0.CSCuz52406	2.0(13) (入手可能)
Cisco Unified Computing System (Management software)	0.CSCuz52483	3.1.2 (AUG-2016)
Cisco Virtual Security Gateway	0.CSCuz52402	5.2(1) (2016年8月20日) VSG2(1.4) (2016年8月20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 190 ATA Series Analog Terminal Adaptor	0.CSCuz52534	1.3.0 (2017年4月)
Cisco 8800 Series IP Phones - VPN Feature	0.CSCuz52565	11.5.2 (2016年12月12日)
Cisco ATA 187 Analog Telephone Adaptor	0.CSCuz52560	9.2.5 (2017年4月5日)
Cisco Agent Desktop for Cisco Unified Contact Center Express	0.CSCuz52539	修正は必要ありません
Cisco Computer Telephony Integration Object Server (CTIOS)	0.CSCuz52360	11.51 (Available)
Cisco DX シリーズ IP フォン	0.CSCuz52563	修正は必要ありません
Cisco Emergency Responder	0.CSCuz52543	11.5 (Available)
Cisco Finesse	0.CSCuz63940	11.5.1 (2016年8月9日)
Cisco Hosted Collaboration Mediation Fulfillment	0.CSCuz52547	10.6(1.99000.17) (入手可能) 10.6(1.99000.18) (入手可能) 10.6(3.11002.7) (入手可能)

Cisco IM and Presence Service (CUPS)	0.CSCuz52545	11.5 (Available)
Cisco IP Interoperability and Collaboration System (IPICS)	0.CSCuz52461	5.0 (2016年8月30日)
Apple iOS向けCisco Jabber	0.CSCuz52550	11.7.0 (入手可能)
Cisco MediaSense	0.CSCuz52562	11.5.1 (入手可能)
Cisco Paging Server (Informacast)	0.CSCuz52548	11.5.1 (入手可能)
Cisco Paging Server	0.CSCuz52548	11.5.1 (入手可能)
Cisco SPA112 2-Port Phone Adapter	0.CSCuz52494	1.4.5 (2016年10月5日)
Cisco SPA122 ATA with Router	0.CSCuz52494	1.4.5 (2016年10月5日)
Cisco SPA232D Multi-Line DECT ATA	0.CSCuz52494	1.4.5 (2016年10月5日)
Cisco SPA30X Series IP Phones	0.CSCuz52496	No further releases are planned
Cisco SPA50X Series IP Phones	0.CSCuz52496	No further releases are planned
Cisco SPA51X Series IP Phones	0.CSCuz52496	No further releases are planned
Cisco SPA525G	0.CSCuz52495	7.6.5 (2017年4月5日)
Cisco Unified 6901 IP フォン	0.CSCuz52557	9.3(1)SR3 (2017年4月5日)
Cisco Unified 6945 IP フォン	0.CSCuz52561	公開済みの修正プログラムはありません
Cisco Unified 7800 Series IP Phones	0.CSCuz52566	11.5.2 (入手可能)
Cisco Unified 8831 シリーズ IP Conference Phone	0.CSCuz52559	79xx:9.4.2 SR2 (2016年6月) 8831: 10.3.2 (2016年7月) 99xx:9.4.2SR3 (2016年7月) 8941/45:9.4.2SR3 (2016年8月)
Cisco Unified 8945 IP フォン	0.CSCuz52558	9.4.2SR3 (入手可能)
Cisco Unified 8961 IP フォン	0.CSCuz52546	9.4.2SR3 (入手可能)
Cisco Unified 9951 IP フォン	0.CSCuz52546	9.4.2SR3 (入手可能)
Cisco Unified 9971 IP フォン	0.CSCuz52546	9.4.2SR3 (入手可能)
Cisco Unified Attendant Console Advanced	0.CSCuz52532	11.5.1 (入手可能)
Cisco Unified Attendant Console Business Edition	0.CSCuz52532	11.5.1 (入手可能)
Cisco Unified Attendant Console	0.CSCuz52532	11.5.1 (入手可能)

Department Edition		
Cisco Unified Attendant Console Enterprise Edition	0.CSCuz52532	11.5.1 (入手可能)
Cisco Unified Attendant Console Premium Edition	0.CSCuz52532	11.5.1 (入手可能)
Cisco Unified Attendant Console Standard	0.CSCuz52533	11.5.1 (入手可能)
Cisco Unified Communications Manager (UCM)	0.CSCuz52535	11.5 (Available)
Cisco Unified Communications Manager Session Management Edition (SME)	0.CSCuz52535	11.5 (Available)
Cisco Unified Communications for Microsoft Lync	0.CSCuz52541	11.6(0.39070) (入手可能)
Cisco Unified Contact Center Enterprise	0.CSCuz52360	11.51 (Available)
Cisco Unified Contact Center Express - Live Data Server	0.CSCuz63936	
Cisco Unified Contact Center Express	0.CSCuz63939	11.5.1 (入手可能)
Cisco Unified IP Conference Phone 8831 for Third-Party Call Control	0.CSCuz52320	No further releases are planned.
Cisco Unified IP Phone 7900 Series	0.CSCuz52567	公開済みの修正プログラムはありません
Cisco Unified Intelligent Contact Management Enterprise	0.CSCuz52360	11.51 (Available)
Cisco Unified Sip Proxy	0.CSCuz52349	CUSP 10.0 (2016年9月)
Cisco Unified Wireless IP Phone	0.CSCuz52573	1.5.1 (2017年4月5日)
Cisco Unified Workforce Optimization Quality Management	0.CSCuz52571	11.0 SR3 ES5 (2016年6月30日)
Cisco Unified Workforce Optimization	0.CSCuz52572	11.0 SR3 ES5 (入手可能)
Cisco Unity Connection (UC)	0.CSCuz52538	11.5 (Available)
Cisco Unity Express	0.CSCuz52348	10.0 (2017年1月)
Cisco Virtualization Experience Media Engine	0.CSCuz52570	11.7(0) (入手可能) 11.5.1 (入手可能)

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)	0.CSCuz52522	9.4.5 (2016年6月30日)
Cisco DCM Series 9900-Digital Content Manager	0.CSCuz52407	19.0.0 (入手可能)
Cisco Digital Media Players (DMP) 4300 Series	0.CSCuz52440	" 5.4(1)RB(2P11) (入手可能) 5.3(6) RB(2P8) (入手可能)
Cisco Digital Media Players (DMP) 4400 Series	0.CSCuz52440	" 5.4(1)RB(2P11) (入手可能) 5.3(6) RB(2P8) (入手可能)
Cisco Edge 300 Digital Media Player	0.CSCuz52514	1.6RB4_5 (2016年6月29日)
Cisco Edge 340 Digital Media Player	0.CSCuz52515	1.2.0.20 (2016年6月23日)
Cisco Enterprise Content Delivery System (ECDS)	0.CSCuz52442	2.6.8 (入手可能)
Cisco Expressway Series	0.CSCuz55590	8.8 (Available)
Cisco Internet Streamer (CDS)	0.CSCuz52465	4.3.2 (2016年6月)
Cisco Media Experience Engines (MXE)	0.CSCuz52449	3.5.2 (入手可能)
Cisco Media Services Interface	0.CSCuz52438	修正は必要ありません
Cisco Show and Share (SnS)	0.CSCuz52454	修正は不要です。
Cisco TelePresence 1310	0.CSCuz52531	" 6.1.13 (2016年1月15日) 1.10.16 (2016年1月15日) 1.9.12 (2016年1月15日)
Cisco TelePresence Conductor	0.CSCuz52439	4.3 (Available)
Cisco TelePresence Content Server (TCS)	0.CSCuz52456	7.2 (Available)
Cisco TelePresence EX Series	0.CSCuz52455	7.3.7 (2016年9月) 8.2.0 (2016年7月)
Cisco TelePresence ISDN GW 3241	0.CSCuz52444	2.2(113) (入手可能)
Cisco TelePresence ISDN GW MSE 8321	0.CSCuz52444	2.2(113) (入手可能)
Cisco TelePresence ISDN Link	0.CSCuz52446	1.1.6 (入手可能)
Cisco TelePresence MCU (8510,	0.CSCuz52447	4.5(1.86) (2016年11月)

8420, 4200, 4500 and 5300)		
Cisco TelePresence MX Series	0.CSCuz52455	7.3.7 (2016年9月) 8.2.0 (2016年7月)
Cisco TelePresence Profile Series	0.CSCuz52455	7.3.7 (2016年9月) 8.2.0 (2016年7月)
Cisco TelePresence SX Series	0.CSCuz52455	7.3.7 (2016年9月) 8.2.0 (2016年7月)
Cisco TelePresence Serial Gateway Series	0.CSCuz52453	修正の予定はありません
Cisco TelePresence Server 8710、7010	0.CSCuz52458	4.2 MR2 (入手可能) 4.4 (Available)
Cisco TelePresence Server on Multiparty Media 310、320	0.CSCuz52458	4.2 MR2 (入手可能) 4.4 (Available)
Cisco TelePresence Server on Virtual Machine	0.CSCuz52458	4.2 MR2 (入手可能) 4.4 (Available)
Cisco TelePresence Supervisor MSE 8050	0.CSCuz52448	2.3(1.50) (入手可能)
Cisco TelePresence System 1000	0.CSCuz52531	" 6.1.13 (2016年1月15日) 1.10.16 (2016年1月15日) 1.9.12 (2016年1月15日)
Cisco TelePresence System 1100	0.CSCuz52531	" 6.1.13 (2016年1月15日) 1.10.16 (2016年1月15日) 1.9.12 (2016年1月15日)
Cisco TelePresence System 1300	0.CSCuz52531	" 6.1.13 (2016年1月15日) 1.10.16 (2016年1月15日) 1.9.12 (2016年1月15日)
Cisco TelePresence System 3000 Series	0.CSCuz52531	" 6.1.13 (2016年1月15日) 1.10.16 (2016年1月15日) 1.9.12 (2016年1月15日)
Cisco TelePresence System 500-32	0.CSCuz52531	" 6.1.13 (2016年1月15日) 1.10.16 (2016年1月15日) 1.9.12 (2016年1月15日)
Cisco TelePresence System 500-	0.CSCuz52531	"

37		6.1.13 (2016年1月15日) 1.10.16 (2016年1月15日) 1.9.12 (2016年1月15日)
Cisco TelePresence TX 9000 Series	0.CSCuz52531	" 6.1.13 (2016年1月15日) 1.10.16 (2016年1月15日) 1.9.12 (2016年1月15日)
Cisco TelePresence Video Communication Server (VCS)	0.CSCuz55590	8.8 (Available)
Cisco Telepresence Integrator C シリーズ	0.CSCuz52455	7.3.7 (2016年9月) 8.2.0 (2016年7月)
Cisco Video Distribution Suite for Internet Streaming (VDS-IS/CDS-IS)	0.CSCuz52464	4.3.2 (2016年6月)
Cisco Video Surveillance 3000 Series IP Cameras	0.CSCuz52490	2.8(0.297) (入手可能)
Cisco Video Surveillance 3000 Series IP Cameras	0.CSCuz52491	2.8(0.297) (入手可能)
Cisco Video Surveillance 4000 Series High-Definition IP Cameras	0.CSCuz52488	2.4(6.309) (入手可能)
Cisco Video Surveillance 4300E/4500E High-Definition IP Cameras	0.CSCuz52489	3.2.8 (2016年5月)
Cisco Video Surveillance 6000 Series IP Cameras	0.CSCuz52490	2.8(0.297) (入手可能)
Cisco Video Surveillance 6000 Series IP Cameras	0.CSCuz52491	2.8(0.297) (入手可能)
Cisco Video Surveillance 7000 Series IP Cameras	0.CSCuz52490	2.8(0.297) (入手可能)
Cisco Video Surveillance 7000 Series IP Cameras	0.CSCuz52491	2.8(0.297) (入手可能)
Cisco Video Surveillance Media Server	0.CSCuz52492	7.9 (2016年12月)
Cisco Video Surveillance PTZ IP Cameras	0.CSCuz52490	2.8(0.297) (入手可能)
Cisco Video Surveillance PTZ IP Cameras	0.CSCuz52491	2.8(0.297) (入手可能)
Cisco Videoscape Control Suite	0.CSCuz52462	影響を受けるシステムは更新されます

		(2016年6月30日)。
Cloud Object Store (COS)	0.CSCuz52463	3.8 (Available)
Tandberg Codian ISDN GW 3210/3220/3240	0.CSCuz52444	2.2(113) (入手可能)
Tandberg Codian MSE 8320 model	0.CSCuz52444	2.2(113) (入手可能)
ワイヤレス		
Cisco Aironet 2700 シリーズ アク セス ポイント	0.CSCuz52410	
Cisco Mobility Services Engine (MSE)	0.CSCuz52422	8.0 (Available)
Cisco Wireless Control System	0.CSCuz73565	修正予定なし.
Cisco Wireless LAN Controller (WLC)	0.CSCuz52435	8.0 MR4 (2016年11月) 8.2 MR1 (2016年7月) 8.3 (2016年6月)
シスコ ホステッド サービス		
Cisco Connected Analytics For Collaboration	0.CSCuz52356	1.0.1q (2016年7月29日)
Cisco Intelligent Automation for Cloud	0.CSCuz52460	0.9.8 (入手可能)
Cisco Proactive Network Operations Center	0.CSCuz52354	3.0.19 (2016年9月)
Cisco Registered Envelope Service (CRES)	0.CSCuz52362	Affected systems have been updated.
Cisco Smart Care	0.CSCuz52473	
Cisco Universal Small Cell 5000 シ リーズ (V3.4.2.x ソフトウェアを 実行)	0.CSCuz52520	3.5.12.21 (2016年6月30日)
Cisco Universal Small Cell 7000 シ リーズ (V3.4.2.x ソフトウェアを 実行)	0.CSCuz52520	3.5.12.21 (2016年6月30日)
Cisco WebEx Meeting Center	0.CSCuz52382	3.9.0.5 (2016年5月25日) 3.9.1 (2016年5月25日)
Cisco WebEx Messenger Service	0.CSCuz52377	Affected systems have been updated
Network Health Framework (NHF)	0.CSCuz52525	No further releases are planned
Network Performance Analytics (NPA)	0.CSCuz52526	No further releases are planned

Services Analytic Platform	0.CSCuz52357	影響を受けるバージョンは更新され ず (2016年7月30日) 。
----------------------------	------------------------------	--

脆弱性を含んでいないことが確認された製品

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

ネットワーク管理とプロビジョニング

- Cisco Configuration Professional
- Cisco Multicast Manager
- Cisco Prime Home
- Cisco Prime Network Registrar IP アドレス マネージャ (IPAM)

Routing and Switching - Enterprise and Service Provider

- Cisco 910 Industrial Router
- Cisco Broadband Access Center Telco Wireless

Unified Computing

- Cisco Unified Computing System B-Series (Blade) Servers

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 Agent Desktop
- Cisco Packaged Contact Center Enterprise
- Cisco TAPI Service Provider (TSP)
- Cisco Unified Communications Domain Manager

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 D9859 Advanced Receiver Transcoder

シスコ ホステッド サービス

- Cisco Cloud Web Security

- Cisco One Portal
- Cisco Services Provisioning Platform (SPP)
- Cisco Universal Small Cell usc-iuh
- Cisco WebEx Meetings (Meeting Center, Training Center, Event Center, Support Center)
- Serial Number Assessment Service (SNAS)
- Small Cell factory recovery root filesystem V2.99.4 or later

詳細

2016年5月3日にOpenSSL Software Foundation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。

OpenSSLの信頼できないASN.1構造の境界外の書き込みの脆弱性

OpenSSLのASN.1エンコーダの脆弱性により、認証されていないリモートの攻撃者が任意のコードを実行したり、サービス妨害(DoS)状態を引き起こしたりする可能性があります。

この脆弱性は、該当するソフトウェアが特定のASN.1データ構造を符号化する方法に起因します。攻撃者は、巧妙に細工された証明書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、該当ソフトウェアがクラッシュしたり、OpenSSLライブラリを使用しているアプリケーションを実行するターゲットユーザの権限で任意のコードが実行されたりする可能性があります。ユーザが特権を昇格すると、エクスプロイトに成功するとシステムが完全に侵害される可能性があります。

本脆弱性の ID は CVE ID CVE-2016-2108 です。

OpenSSL AES CBC暗号のman-in-the-middle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を復号化して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十分なパディングチェックに起因します。攻撃者は、ターゲットシステムと、Advanced Encryption Standards New Instructions(AES-NI)をサポートするTransport Layer Security/Secure Sockets Layer(TLS/SSL)またはDatagram Transport Layer Security(DTLS)サーバとの間で中間者の位置にあり、接続にAES Cipher Block Chaining(CBC)暗号が使用されている場合、padding oracle攻撃を実行することで、この脆弱性を不正利用できます。エクスプロイトに成功すると、攻撃者は暗号化されたパケットの機密情報を復号化し、さらなる攻撃に利用できる可能性があります。

本脆弱性の ID は CVE ID CVE-2016-2107 です。

OpenSSL EVP_EncryptUpdate関数のオーバーフローによるヒープ破損の脆弱性

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任意のコードを実行したり、ターゲットシステムでサービス妨害(DoS)状態を引き起こしたりす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ユーザ入力の検証が不適切なことに起因します。攻撃者は、巧妙に細工された大量のデータを該当ソフトウェアの EVP_EncryptUpdate()関数に送信することで、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、攻撃者はユーザの権限で任意のコードを実行したり、ターゲットシステムでDoS状態を引き起こしたりする可能性があります。

本脆弱性の ID は CVE ID CVE-2016-2106 です。

OpenSSL EVP_EncodeUpdate関数のオーバーフローの脆弱性

OpenSSLの EVP_EncodeUpdate()関数の脆弱性により、認証されていないリモートの攻撃者が任意のコードを実行したり、サービス妨害(DoS)状態を引き起こしたりす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境界チェックが不十分であることに起因します。攻撃者は、ターゲットシステムでOpenSSLライブラリを使用するアプリケーションに大量のデータを送信することで、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、オーバーフロー状態が引き起こされ、ヒープが破損する可能性があります。攻撃者は、ヒープの破損を使用して、アプリケーションを実行しているユーザのセキュリティコンテキストで、アプリケーションをクラッシュさせたり、任意のコードを実行したりする可能性があります。ユーザが昇格された特権でアプリケーションを実行している場合、攻撃者はこれらの特権で任意のコードを実行し、システムを完全に侵害する可能性があります。

本脆弱性の ID は CVE ID CVE-2016-2105 です。

OpenSSL d2i_CMS_bio関数のDoS脆弱性

OpenSSLの脆弱性により、ローカル攻撃者がターゲットシステムでサービス拒否(DoS)状態を引き起こす可能性があります。

この脆弱性は、特定のデータの処理中にメモリが枯渇することに起因します。攻撃者は、巧妙に細工されたASN.1データをターゲットシステムに送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、過剰なメモリリソースの消費が引き起こされ、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-2016-2109 です。

OpenSSL ASN.1ストリングX509_NAME_oneline関数の読み取り過多の脆弱性

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、該当ソフトウェアによる不適切なメモリプロセスに起因します。攻撃者は、1004バイトを超える巧妙に細工されたASN.1ストリングを該当ソフトウェアのX509_NAME_oneline()関数に送信することで、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、攻撃者はメモリのオーバーリード状態を引き起こし、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-2016-2176 です。

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/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」セクションで製品を特定した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。

推奨事項

\$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) 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やその公表を確認していません。

出典

これらの脆弱性は、2016年5月3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-20160504-openssl>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.12	脆弱性のある製品のリストを更新。	脆弱性が存在する製品	Final	2016年 12月5日
1.11	脆弱な製品のリストと脆弱性のない製品を更新。	「脆弱性のある製品」、「脆弱性を含んでいないことが確認された製品」	Final	2016年 11月8日

バージョン	説明	セクション	ステータス	日付
1.10	脆弱性のある製品のリストを更新。	脆弱性が存在する製品	Final	2016年7月22日
1.9	脆弱性のある製品のリストを更新。	脆弱性が存在する製品	Final	2016年6月29日
1.8	調査中の製品、脆弱性のある製品、脆弱性を含ま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, 脆弱性を含まないことが確認された製品	Final	2016年6月22日
1.7	調査中の製品、脆弱性のある製品、脆弱性を含ま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, 脆弱性を含まないことが確認された製品	Interim	2016 月 6 月 1 日
1.6	調査中の製品、脆弱性のある製品、脆弱性を含ま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, 脆弱性を含まないことが確認された製品	Interim	2016年5月17日
1.5	調査中の製品、脆弱性のある製品、脆弱性を含ま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, 脆弱性を含まないことが確認された製品	Interim	2016年5月13日
1.4	調査中の製品、脆弱性のある製品、脆弱性を含ま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, 脆弱性を含まないことが確認された製品	Interim	2016年5月10日
1.3	調査中の製品、脆弱性のある製品、脆弱性を含ま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, 脆弱性を含まないことが確認された製品	Interim	2016年5月9日
1.2	調査中の製品、脆弱性のある製品、脆弱性を含ま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, 脆弱性を含まないことが確認された製品	Interim	2016年5月6日
1.1	調査中の製品、脆弱性のある製品、脆弱性を含ま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, 脆弱性を含まないことが確認された製品	Interim	2016年5月5日
1.0	初回公開リリース	—	Interim	2016年5月4日

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。

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。