シスコ製品に影響する OpenSSL の複数の脆弱性（2016 年 1 月）

High

アドバイザリーID : cisco-sa-20160129-openssl

初公開日 : 2016-01-29 16:00

最終更新日 : 2018-01-04 12:43

バージョン 1.15 : Final

回避策 : No workarounds available

Cisco バグ ID : CSCuy07470 CSCuy07492 CSCuy07294 CSCuy16302 CSCuy07316 CSCuy07438 CSCuy07517 CSCuy07319 CSCuy07372 CSCuy07230 CSCuy07231 CSCuy07452 CSCuy07476 CSCuy07355 CSCuy07478 CSCuy16299 CSCuy07469 CSCuy07524 CSCuy07305 CSCuy07208 CSCuy07329 CSCuy07508 CSCuy07408 CSCuy07363 CSCuy07342 CSCuy07288 CSCuy07520 CSCuy07223 CSCuy07267 CSCuy07289 CSCuy07467 CSCuy07225 CSCuy07247

CVE-2015-3197 CVE-2016-0701

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 1 月 28 日、OpenSSL Project は 2 つの脆弱性について詳述したセキュリティ アドバイザリを公開しました。

1 つ以上の脆弱性の影響を受ける OpenSSL パッケージのバージョンが複数のシスコ製品に組み込まれています。これにより、未認証のリモート攻撃者が SSL/TLS 接続で中間者攻撃を実施する可能性があります。

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。

シスコでは、これらの脆弱性に対するソフトウェア アップデートを提供する予定です。

これらの脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160129-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の製品ラインの調査を完了しています。 このバグは Cisco Bug Search Tool で検索でき、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入手可能です。

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脆弱性の影響を受けるシスコ製品を示します。

Product	Cisco Bug ID	Fixed Release Availability
Collaboration and Social Media		
Cisco WebEx Meetings Server versions 1.x	CSCuy07247	2.6 (April 2016)
Cisco WebEx Meetings Server versions 2.x	CSCuy07247	2.6 (April 2016)
Endpoint Clients and Client Software		
Cisco Jabber for Windows	CSCuy07508	11.6 (Apr-6 2016)
Network and Content Security Devices		
Cisco ASA Next-Generation Firewall Services	CSCuy07392	
Cisco Email Security Appliance (ESA)	CSCuy07231	
Cisco IPS	CSCuy07438	7.1(11) (March 2016) 7.3(05) (Apr 2016)
Network Management and Provisioning		
Cisco Cloupia Unified Infrastructure Controller	CSCuy07267	5.4.0.3 (31-March-2016)
Cisco Prime Collaboration Deployment	CSCuy07476	11.5 (June 2016)
Cisco Prime Collaboration Provisioning	CSCuy07329	11.5 (Jun 2016)
Cisco Prime License Manager	CSCuy07355	11.5 (June 2016)
Cisco Prime Optical for SPs	CSCuy07316	10.6 (May 2016) 10.5.0.2 パッチ リリース（2016 年 2 月
Cisco Prime Performance Manager	CSCuy07305	1.7.0.4 (29-Apr-2016)
Cisco Unified Intelligence Center（UIC）	CSCuy16299	11.5 (June 2016)
Routing and Switching - Enterprise and Service Provider		
Cisco MDS 9000 Series Multilayer Switches	CSCuy07280	7.3 (May2016)
Cisco Nexus 3000 Series Switches	CSCuy07288	修正プログラムを提供予定（2016 年 4
Cisco Nexus 3X00 シリーズ スイッチ	CSCuy07289	2016 年 4 月に修正プログラムを提供予
Cisco Nexus 5000 Series Switches	CSCuy07280	7.3 (May2016)
Cisco Nexus 6000 Series Switches	CSCuy07280	7.3 (May2016)
Cisco Nexus 7000 Series Switches	CSCuy07280	7.3 (May2016)
Cisco Nexus 9000 シリーズ（スタンドアロン、NxOS を実行）	CSCuy07282	
Cisco ONS 15454 Series Multiservice Provisioning Platforms	CSCuy07408	10.6 (May 2016)

Unified Computing		
Cisco Unified Computing System B-Series (Blade) Servers	CSCuy07294	2.2.(3d) (Feb 2016)
Voice and Unified Communications Devices		
Cisco 8800 Series IP Phones - VPN Feature	CSCuy07524	11.5.0(Apr 2016)
Cisco Agent Desktop	CSCuy07223	11.51 (June 2016)
Cisco Computer Telephony Integration Object Server (CTIOS)	CSCuy07225	11.51 (June 2016)
Cisco Emergency Responder	CSCuy07492	11.5 (June 2016)
Cisco IM and Presence Service (CUPS)	CSCuy07496	11.5 (Jun 2016)
Cisco MediaSense	CSCuy07520	11.5 (15-Jun 2016)
Cisco Unified 8945 IP フォン	CSCuy07517	影響を受けるリリースのパッチ ファイル 2016 年 6 月に提供予定。
Cisco Unified Attendant Console Advanced	CSCuy07469	2016 年 9 月にパッチを提供予定
Cisco Unified Attendant Console Business Edition	CSCuy07469	2016 年 9 月にパッチを提供予定
Cisco Unified Attendant Console Department Edition	CSCuy07469	2016 年 9 月にパッチを提供予定
Cisco Unified Attendant Console Enterprise Edition	CSCuy07469	2016 年 9 月にパッチを提供予定
Cisco Unified Attendant Console Premium Edition	CSCuy07469	2016 年 9 月にパッチを提供予定
Cisco Unified Attendant Console Standard	CSCuy07470	現在パッチ ファイルが利用可能。 CDE 参照してください。
Cisco Unified Communications Manager (UCM)	CSCuy07473	11.5 (Jun 2016)
Cisco Unified Communications Manager Session Management Edition (SME)	CSCuy07473	11.5 (Jun 2016)
Cisco Unified Contact Center Enterprise	CSCuy07225	11.51 (June 2016)
Cisco Unified Contact Center Express - Live Data Server	CSCuy16302	11.51 (June 2016)
Cisco Unified Contact Center Express	CSCuy16304	11.5(1) (June 2016)
Cisco Unified Intelligent Contact Management Enterprise	CSCuy07225	11.51 (June 2016)
Cisco Unity Connection (UC)	CSCuy07478	11.5 (29-Feb 2016)
Cisco Unity Express	CSCuy07208	10.0 (Feb 2017)
test2	CSCuy07489	
Video, Streaming, TelePresence, and Transcoding Devices		
Cisco AnyRes Live (CAL)	CSCuy07452	9.6.3 (11-Feb 2016)
Cisco Edge 300 Digital Media Player	CSCuy07442	1.6RB4_4 (March 2016)
Cisco Expressway Series	CSCuy07363	X8.7.2 (March 2016)
Cisco TelePresence 1310	CSCuy07467	2016 年 7 月に修正プログラムを提供予
Cisco TelePresence Conductor	CSCuy07342	XC 4.2 (March 2016)
Cisco TelePresence System 1000	CSCuy07467	2016 年 7 月に修正プログラムを提供予
Cisco TelePresence System 1100	CSCuy07467	2016 年 7 月に修正プログラムを提供予
Cisco TelePresence System 1300	CSCuy07467	2016 年 7 月に修正プログラムを提供予
Cisco TelePresence System 3000 Series	CSCuy07467	2016 年 7 月に修正プログラムを提供予
Cisco TelePresence System 500-32	CSCuy07467	2016 年 7 月に修正プログラムを提供予
Cisco TelePresence System 500-37	CSCuy07467	2016 年 7 月に修正プログラムを提供予
Cisco TelePresence TX 9000 Series	CSCuy07467	2016 年 7 月に修正プログラムを提供予
Cisco TelePresence Video Communication Server (VCS)	CSCuy07363	X8.7.2 (March 2016)
Cisco Videoscape Control Suite	CSCuy07372	3.5.3 (29-Feb 2016)
Wireless		

Cisco Mobility Services Engine（MSE）	CSCuy07319	8.0.140.0. (31-March-2016)
シスコ クラウド ホステッド サービス		
Cisco Proactive Network Operations Center	CSCuy07216	修正プログラムを提供予定（2016 年 3 日）
Cisco Registered Envelope Service（CRES）	CSCuy07230	4.7 (March 2016)
Cisco WebEx Messenger Service	CSCuy07254	Affected systems have been updated.

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記載された脆弱性の影響を受けません。

ケーブル モデム

- Cisco Unified 6921 IP フォン

Collaboration and Social Media

- Cisco SocialMiner
- 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 OS X
- Cisco AnyConnect Secure Mobility Client for Windows
- Cisco AnyConnect Secure Mobility Client for iOS
- Cisco Jabber Guest 10.0(2)
- Cisco Jabber Software Development Kit
- Cisco Jabber for Android
- Cisco Jabber for Mac
- Cisco Jabber for iOS
- Cisco MMP サーバ
- Cisco WebEx Connect クライアント（Windows）
- Cisco WebEx Meetings Client - Hosted
- Cisco WebEx Meetings Client - On Premises
- Cisco WebEx Meetings for Android
- Cisco WebEx Meetings for Blackberry
- Cisco WebEx Meetings for WP8
- Cisco WebEx Productivity Tools
- WebEx Recording Playback Client

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

- Cisco ACE 4710 Application Control Engine（A5）
- Cisco Application and Content Networking System（ACNS）
- Cisco InTracer
- Cisco Network Admission Control (NAC)
- 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 CX と Cisco Prime Security Manager
- Cisco ASA Content Security and Control（CSC）Security Services Module
- Cisco Adaptive Security Appliance（ASA）
- Cisco Clean Access Manager
- Cisco Content Security Appliance Updater Servers
- Cisco Content Security Management Appliance (SMA)
- Cisco FireSIGHT システム ソフトウェア
- Cisco Identity Services Engine（ISE）
- Cisco IronPort Encryption Appliance（IEA）
- Cisco NAC Guest Server
- Cisco NAC Server
- Cisco Physical Access Control Gateway
- Cisco Secure Access Control Server（ACS）
- Cisco Secure Access Control System（ACS）
- Cisco Virtual Security Gateway for Microsoft Hyper-V
- Cisco Web Security Appliance (WSA)

ネットワーク管理とプロビジョニング

- Cisco Application Networking Manager
- Cisco Application Policy Infrastructure Controller（APIC）
- Cisco Configuration Professional
- Cisco Digital Media Manager
- Cisco MATE Collector
- Cisco MATE Design
- Cisco MATE Live
- Cisco Management Appliance (MAP)
- Cisco Mobile Wireless Transport Manager
- Cisco Multicast Manager
- Cisco NetFlow Generation Appliance
- Cisco Network Analysis Module
- Cisco Packet Tracer

- Cisco Prime Access Registrar
- Cisco Prime Collaboration Assurance
- Cisco Prime Data Center Network Manager（DCNM）
- Cisco Prime Home
- Cisco Prime IP Express
- Cisco Prime Infrastructure Standalone Plug and Play Gateway
- Cisco Prime Infrastructure
- Cisco Prime LAN Management Solution（LMS - Solaris）
- Cisco Prime Network Registrar（PNR）
- Cisco Prime Network Registrar IP アドレス マネージャ（IPAM）
- Cisco Prime Network Services Controller
- Cisco Prime Network
- Cisco Prime Security Manager
- Cisco Quantum Policy Suite (QPS)
- Cisco Quantum SON Suite（Cisco Quantum SON スイート）
- Cisco Security Manager
- Cisco UCS Central
- Local Collector Appliance（LCA）

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 910 Industrial Router
- Cisco ASR 5000 シリーズ
- Cisco Broadband Access Center Telco Wireless
- Cisco Connected Grid Router - CGOS
- Cisco Connected Grid ルータ
- Cisco IOS ソフトウェアと Cisco IOS-XE ソフトウェア
- Cisco IOS-XE（SSLVPN 機能）
- Cisco IOS-XE（WebUI 機能のみ）
- Cisco IOS-XR
- Cisco Nexus 1000V InterCloud
- Cisco Nexus 1000V シリーズ スイッチ（ESX）
- Cisco Nexus 1000V シリーズ スイッチ
- Microsoft Hyper-V 向け Cisco Nexus 1000V スイッチ
- Cisco Nexus 4000 Series Blade Switches
- Cisco Nexus 9000 (ACI/Fabric Switch)
- Cisco OnePK All-in-One VM
- 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 Sx220 switches

- Cisco Sx300 switches
- Cisco Sx500 switches

Unified Computing

- Cisco Common Services Platform Collector
- Cisco Standalone ラック サーバ CIMC
- Cisco UCS Invicta Series Solid State Systems
- Cisco Unified Computing System (Management software)
- 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 190 ATA Series Analog Terminal Adaptor
- Cisco 7937 IP Phone
- Cisco ATA 187 Analog Telephone Adaptor
- Cisco Agent Desktop for Cisco Unified Contact Center Express
- Cisco DX シリーズ IP フォン
- Cisco Finesse
- Cisco Hosted Collaboration Mediation Fulfillment
- Cisco IP Interoperability and Collaboration System (IPICS)
- Cisco MeetingPlace
- Cisco Packaged Contact Center Enterprise
- Cisco Paging Server（Informacast）
- Cisco Paging Server
- Cisco Remote Silent Monitoring
- Cisco SPA112 2-Port Phone Adapter
- Cisco SPA122 ATA with Router
- Cisco SPA232D Multi-Line DECT ATA
- Cisco SPA30X Series IP Phones
- Cisco SPA50X Series IP Phones
- Cisco SPA51X Series IP Phones
- Cisco SPA525G
- Cisco SPA8000 8 ポート IP テレフォニー ゲートウェイ
- Cisco SPA8800 IP テレフォニー ゲートウェイ（4 FXS ポートと 4 FXO ポートを内蔵）
- Cisco TAPI Service Provider（TSP）
- Cisco Unified 6901 IP フォン
- Cisco Unified 6945 IP フォン
- Cisco Unified 7800 Series IP Phones
- Cisco Unified 8831 シリーズ IP Conference Phone
- Cisco Unified 8961 IP フォン
- Cisco Unified 9951 IP フォン

- Cisco Unified 9971 IP フォン
- Cisco Unified Communications Domain Manager
- Cisco Unified Communications for Microsoft Lync
- Cisco Unified E-Mail Interaction Manager
- Cisco Unified IP Conference Phone 8831 for Third-Party Call Control
- Cisco Unified IP Phone 7900 Series
- Cisco Unified Sip Proxy
- Cisco Unified Web Interaction Manager
- Cisco Unified Wireless IP Phone
- Cisco Unified Workforce Optimization Quality Management
- Cisco Unified Workforce Optimization
- Cisco Virtual PGW 2200 ソフトスイッチ
- Cisco Virtualization Experience Media Engine
- Cisco Voice Portal

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
- Cisco D9859 Advanced Receiver Transcoder
- Cisco DCM Series 9900-Digital Content Manager
- Cisco Digital Media Players (DMP) 4300 Series
- Cisco Digital Media Players (DMP) 4400 Series
- Cisco Edge 340 Digital Media Player
- Cisco Enterprise Content Delivery System (ECDS)
- Cisco Headend System Release
- Cisco Media Experience Engines（MXE）
- Cisco Media Services Interface
- Cisco Model D9485 DAVIC QPSK
- Cisco Show and Share（SnS）
- Cisco TelePresence Content Server（TCS）
- Cisco TelePresence EX Series
- Cisco TelePresence ISDN GW 3241
- Cisco TelePresence ISDN GW MSE 8321
- Cisco TelePresence ISDN Link
- Cisco TelePresence MCU (8510, 8420, 4200, 4500 and 5300)
- Cisco TelePresence MX Series
- Cisco TelePresence Profile Series
- Cisco TelePresence SX Series
- Cisco TelePresence Serial Gateway Series
- Cisco TelePresence Server 8710、7010
- Cisco TelePresence Server on Multiparty Media 310、320
- Cisco TelePresence Server on Virtual Machine

- Cisco TelePresence Supervisor MSE 8050
- Cisco Telepresence Integrator C
- Cisco VEN501 Wireless Access Point
- 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 4300E/4500E High-Definition IP Cameras
- Cisco Video Surveillance 6000 Series IP Cameras
- Cisco Video Surveillance 7000 Series IP Cameras
- Cisco Video Surveillance Media Server
- Cisco Video Surveillance PTZ IP Cameras
- Cloud Object Store（COS）
- Tandberg Codian ISDN GW 3210/3220/3240
- Tandberg Codian MSE 8320 model

ワイヤレス

- Cisco Aironet 2700 シリーズ アクセス ポイント
- Cisco Wireless LAN Controller（WLC）

シスコ クラウド ホステッド サービス

- Cisco Cloud Web Security
- Cisco Connected Analytics For Collaboration
- Cisco Intelligent Automation for Cloud
- Cisco One Portal
- Cisco Services Provisioning Platform（SPP）
- Cisco Smart Care
- Cisco SmartConnection
- Cisco SmartReports
- Cisco UCS Invicta Series Autosupport Portal
- Cisco Unified Services Delivery Platform（USDP）
- Cisco Universal Small Cell 5000 シリーズ（V3.4.2.x ソフトウェアを実行）
- Cisco Universal Small Cell 7000 シリーズ（V3.4.2.x ソフトウェアを実行）
- Cisco Universal Small Cell usc-iuh
- Cisco WebEx Meeting Center
- Cisco WebEx Meetings (Meeting Center, Training Center, Event Center, Support Center)
- 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、シスコ ユニファイド コミュニケーション アップグレード レディネス アセスメント
- Life Cycle Management Agent Manager（LCM）
- Network Health Framework (NHF)
- Network Performance Analytics (NPA)

- Partner Supporting Service（PSS）1.x
- Serial Number Assessment Service（SNAS）
- Services Analytic Platform
- Small Cell factory recovery root filesystem V2.99.4 or later

詳細

2016 年 1 月 28 日に発表された OpenSSL Project の脆弱性の名称およびそれに関連する Common Vulnerabilities and Exposures（CVE）ID は次のとおりです。

OpenSSL における DH 小サブグループの脆弱性

OpenSSL における安全でない素数に基づく Diffie-Hellman（DH）パラメータ生成の脆弱性により、未認証のリモート攻撃者に TLS サーバのプライベート DH 指数を発見されてしまう可能性があります。

この脆弱性は、OpenSSL のバージョン 1.0.2 で導入された、安全でない素数に基づいて DH パラメータを生成する機能に起因するものです。このバージョンでは、X9.42 スタイルのパラメータファイル生成がサポートされています。 この脆弱性は、ピアが同じプライベート DH 指数を使用したハンドシェイクを複数回完了することで、悪用される可能性があります。 悪用されると、TLS サーバのプライベート DH 指数が発見され、SSL/TLS 接続で中間者攻撃を実施される可能性があります。

本脆弱性の ID は CVE ID CVE-2016-0701 です。

OpenSSL SSLv2 において無効化された暗号がブロックされない

OpenSSL の SSL ネゴシエーションにおける脆弱性により、サーバで無効化されている SSLv2 暗号とのネゴシエーションを、未認証のリモート攻撃者に実施されてしまう可能性があります。

この脆弱性は、SSLv2 暗号がすべて無効になっている場合でも、悪意のあるクライアントがサーバで無効化された SSLv2 暗号とのネゴシエーションを実施して SSLv2 ハンドシェイクを完了できることによるものです。 悪用されると、脆弱な SSLv2 暗号とのネゴシエーションを実施されて SSL/TLS 接続を開始され、中間者攻撃に対して脆弱な状態になってしまう可能性があります。

本脆弱性の ID は CVE ID CVE-2015-3197 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、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/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。

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やその公表を確認していません。

出典

本脆弱性は、2016 年 1 年 28 日に OpenSSL Project によって公開されました。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160129-openssl

改訂履歴

Version	Description	Section	Status	日付
1.15	影響を受ける製品のセクションに Cisco Unified Intelligence Center（UIC）を追加。	該当製品	Final	2018-January-04
1.14	調査中の製品、脆弱性がないと確認された製品、脆弱性があると確認された製品に関する情報を更新。	該当製品	Final	2016-March-24
1.13	調査中の製品、脆弱性がないと確認された製品、脆弱性があると確認された製品に関する情報を更新。	該当製品	Interim	2016 年 3 月 2 日
1.12	調査中の製品、脆弱性がないと確認された製品、脆弱性があると確認された製品に関する情報を更新。	該当製品	Interim	2016 年 2 月 25 日
1.11	調査中の製品、脆弱性がないと確認された製品、脆弱性があると確認された製品に関する情報を更新。	該当製品	Interim	2016-February-22
1.10	調査中の製品、脆弱性がないと確認された製品、脆弱性があると確認された製品に関する情報を更新。	該当製品	Interim	2016-February-19
1.9	調査中の製品、脆弱性がないと確認された製品、脆弱性があると確認された製品に関する情報を更新。	該当製品	Interim	2016-February-16
1.8	調査中の製品、脆弱性がないと確認された製品、脆弱性があると確認された製品に関する情報を更新。	該当製品	Interim	2016-February-12
1.7	調査中の製品、脆弱性がないと確認された製品、脆弱性があると確認された製品に関する情報を更新。	該当製品	Interim	2016-February-11
1.6	調査中の製品、脆弱性がないと確認された製品、脆弱性があると確認された製品に関する情報を更新。	該当製品	Interim	2016-February-09
1.5	調査中の製品、脆弱性がないと確認された製品、脆弱性があると確認された製品に関する情報を更新。	該当製品	Interim	2016-February-08
1.4	調査中の製品、脆弱性がないと確認された製品、脆弱性があると確認された製品に関する情報を更新。	該当製品	Interim	2016-February-05
1.3	調査中の製品、脆弱性がないと確認された製品、脆弱性があると確認された製品に関する情報を更新。	該当製品	Interim	2016-February-04
1.2	調査中の製品、脆弱性がないと確認された製品、脆弱性があると	該当	Inte	2016-

	確認された製品に関する情報を更新。	製品	rim	February-03
1.1	調査中の製品、脆弱性がないと確認された製品、脆弱性があると確認された製品に関する情報を更新。	該当製品	Interim	2016-February-02
1.0	初回公開リリース		Interim	2016-January-29

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。