# シスコ製品に影響を及ぼす OpenSSL の多重 脆弱点

Critical

**アドバイザリーID :** cisco-sa-20140605-openssl

**初公開日 :** 2014-06-05 22:40

**最終更新日 :** 2015-03-27 19:50

**バージョン 1.28 :** Final

**CVSSスコア :** 10.0

**回避策 :** No Workarounds available

**Cisco バグ ID :** CSCup22590

CVE-2014-3470
CVE-2014-0195
CVE-2014-0198
CVE-2010-5298
CVE-2014-0076
CVE-2014-0221
CVE-2014-0224

**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

複数のシスコ製品は任意のコードを実行するか、サービス拒否（DoS）状態を作成するか、または man-in-the-middle攻撃を行うために非認証を可能にする可能性がある 1つ以上の脆弱性リモート攻撃者から影響を受ける OpenSSL パッケージのバージョンを織込んでいます。 2014 年 6月 5 日で、OpenSSL プロジェクトは 7 個別の脆弱性を詳述する Security Advisory をリリースしました。 脆弱性はこの文書で次の通り参照されます:

- SSL/TLS マン・イン・ザ・ミドル脆弱性
- DTLS 再帰欠陥脆弱性
- DTLS 無効なフラグメント脆弱性
- SSL_MODE_RELEASE_BUFFERS ヌルポインタ参照解除脆弱性

- SSL_MODE_RELEASE_BUFFERS セッション インジェクトかサービス拒否の脆弱性
- 匿名 ECDH サービス拒否の脆弱性
- ECDSA NONCE 側チャネル リカバリ不正侵入脆弱性

以下の事項に注意して下さい:この脆弱性から影響を受けるデバイスは SSL または DTLS 接続を終える Secure Sockets Layer（SSL）またはデータグラムの転送層としてセキュリティ機能するデバイス（DTLS）SSL または DTLS 接続を開始している SSL クライアントとして機能するサーバまたはデバイスです。 SSL または DTLS トラフィックによってそれを終えないで単に横断されるデバイスは影響を受けていません。

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。

本脆弱性を軽減する回避策が入手できる場合もあります。

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-20140605-openssl

### 該当製品

下記の例に現在リストされていない製品について尋ねたい顧客は Cisco TAC かサポート プロバイダーに連絡し、TAC ケースをオープンする必要があります。

## 脆弱性のある製品

*Collaboration and Social Media*

- Cisco SocialMiner（CSCup24081）
- Cisco WebEx Meetings サーバ バージョン 1.x（CSCup22555）
- Cisco WebEx Meetings サーバ バージョン 2.x（CSCup22555）
- Cisco WebEx Node for MCS（CSCup34787）

*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*

- OpenFlow（CSCup24058）のための Cisco エージェント
- Android（CSCup22547）のための Cisco AnyConnect セキュア モビリティ クライアント
- デスクトップ プラットフォーム（CSCup22547）のための Cisco AnyConnect セキュア モビリティ クライアント
- iOS（CSCup22547）のための Cisco AnyConnect セキュア モビリティ クライアント
- Cisco Jabber for Android（CSCup23952）
- iOS（CSCup23957）のための Cisco Jabber
- Cisco Jabber for Mac（CSCup23910）
- Cisco Jabber Guest（CSCup65216）
- Cisco Jabber ソフトウェア開発キット（CSCup23934）
- Cisco Jabber Video for TelePresence（Movi）（CSCup24126）

- Cisco Jabber Video for iPad（CSCup23942）
- Cisco Jabber Voice for Android（CSCup23938）
- Cisco Jabber Voice for iPhone（CSCup23948）
- Cisco Jabber for Windows（CSCup23913）
- Windows（CSCup23973）のための Cisco WebEx 接続応答 クライアント
- Cisco WebEx Meetings サーバ（クライアント）（CSCup22614）
- ブラックベリー（CSCup22617）のための Cisco WebEx Meetings
- Cisco WebEx 生産性ツール（CSCup22568）

*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 アプリケーション コントロール エンジン モジュール（ACE10、ACE20）（CSCup28056）
- Cisco ACE アプリケーション コントロール エンジン モジュール（ACE30）（CSCup22544）
- Cisco ACE アプリケーション制御エンジン アプライアンス（ACE4710）（CSCup22544）
- Cisco Wide Area Application Services（WAAS）アプライアンス（WAAS）（CSCup22648）

*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 適応型セキュリティ アプライアンス（ASA）ソフトウェア（CSCup22532）
- Cisco ASA CX コンテキストわかっているセキュリティ（CSCup24314）
- Cisco コンテンツ セキュリティ管理アプライアンス（SMA）（CSCup22506）
- Cisco E メール セキュリティ アプライアンス（ESA）（CSCup21571）
- Cisco NAC アプライアンス（Clean Access）（Clean Access サーバ）（CSCup24014）
- Cisco NAC マネージャ（Clean Access Manager）（CSCup24028）
- Cisco NAC Guest Server（CSCup24002）
- Cisco IPS（CSCup22652）
- Cisco 識別 サービス エンジン（ISE）（CSCup22534）
- Cisco Physical Access Gateway（CSCup22414）
- Cisco Secure Access Control Server（ACS）（CSCup22665）
- Cisco Small Business ISA500 シリーズ統合型セキュリティ アプライアンス（CSCup24029）
- 超V Microsoft のための Cisco Virtual Security Gateway（CSCup22419）
- VMware（CSCup22419）のための Cisco Virtual Security Gateway
- Cisco Web セキュリティ アプライアンス（WSA）（CSCup22522）

*ネットワーク管理とプロビジョニング*

- Cisco Application Policy Infrastructure Controller（APIC）（APIC）（CSCup22625）

- Cisco Application Networking Manager（ANM）（CSCup24492）
- Common Services Platform Collector（CSPC）Cisco（CSCup24136）
- Cisco 仲間製品（CSCup22446）
- Cisco Prime Access Registrar（CSCup23967）
- Cisco Prime Collaboration 配備（CSCup23962）
- 10.5 を提供する Cisco Prime Collaboration（CSCup23964）
- Cisco Prime Data Center Network Manager（DCNM）（CSCup22646）
- Cisco Prime Infrastructure（CSCup22623）
- Cisco Prime IP Express（CSCup39248）
- Cisco Prime LAN Management Solution（LMS）（CSCup22054）
- Cisco Prime LAN Management Solution（LMS）- Solaris（CSCus55522）
- Cisco Prime License Manager（CSCup23915）
- Cisco Prime Network（CSCup22047）
- Cisco Prime Network Analysis Module（NAM）アプライアンス（NAM）（CSCup24103）
- Cisco Prime Network Services Controller（PNSC）（CSCup22613）
- Cisco Prime Network Registrar（CPNR）（CSCup22498）
- SPS（CSCup22035）のための Cisco Prime Optical
- SPS（CSCup22038）のための Cisco Prime Performance Manager
- Cisco Quantum Policy Suite（QPS）（CSCup24089）
- Cisco Security Manager（CSCup22582）
- Ciscoネットワーク Registar（CSCup44973）のためのセキュリティモジュール

*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 1000 シリーズ Connected Grid ルータ（CSCup24084）
- Cisco CSS 11500 シリーズ コンテンツ サービス スイッチ（CSCup28017）
- Cisco IOSソフトウェア（CSCup22590）
- Cisco IOS XE ソフトウェア（CSCup22487）
- Cisco IOS XR ソフトウェア（CSCup22654）
- Cisco MDS は切り替えます（CSCup22563）
- Cisco METRO イーサネット 1200 シリーズ アクセスデバイス（CSCup70117）
- Cisco MXE 3500 シリーズ（Media Experience Engines）（CSCup22361）
- Cisco MXE 5600 シリーズ（CSCup2236）
- Cisco Nexus 1000V InterCloud（CSCup22571）
- Microsoft Hyper-V 向け Cisco Nexus 1000V スイッチ（CSCup23937）
- VMware vSphere 向け Cisco Nexus 1000V スイッチ（CSCup22641）
- Cisco Nexus 1010 Virtual Services Appliance（CSCup22643）
- Cisco Nexus 1100 バーチャル サービス アプライアンス（CSCup22643）
- Cisco Nexus 2000 シリーズ ファブリック エクステンダ（CSCup22365）（CSCup22663）
- Cisco Nexus 3000 シリーズ スイッチ（CSCup44235）

- Cisco Nexus 3164 スイッチ（CSCup24057）
- Cisco Nexus 5000 シリーズ スイッチ（CSCup22365）（CSCup22663）
- Cisco Nexus 5600 シリーズは切り替えます（CSCup22365）（CSCup22663）
- Cisco Nexus 6000 シリーズ スイッチ（CSCup22365）（CSCup22663）
- Cisco Nexus 7000 シリーズ スイッチ（CSCup22563）
- Cisco Nexus 9000 シリーズ スイッチ（CSCup24057）
- Cisco OnePK オールインワン VM（CSCup22592）
- Cisco ONS 15400 シリーズ（CSCup24077）

*ルーティングおよびスイッチング - スモール ビジネス*

- Cisco RV180W ワイヤレスN VPN Router（CSCuo18692）
- Cisco RV220W ワイヤレスN VPN Router（CSCuo18692）
- VoIP（CSCup22426）の Cisco WAG310G ワイヤレスG ADSL2+ ゲートウェイ

*Unified Computing*

- Cisco UCS B シリーズ（ブレード）サーバ（CSCup22565）
- Cisco UCS Cシリーズ（スタンドアロン ラック）サーバ（CSCup22566）
- Cisco UCS 本部（CSCup22584）
- Cisco UCS ファブリックは相互接続します（CSCup53743）
- Cisco UCS Invicta シリーズ ソリッドステート システム（CSCup22388）

*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 D9036 モジュラ エンコード プラットフォーム（CSCup23995）
- Cisco Digital Media Manager（DMM）（CSCup24174）
- Cisco Edge 300 デジタル メディア プレーヤー（CSCup24260）
- Cisco Edge 340 デジタル メディア プレーヤー（CSCup24248）
- Cisco Digital Media Player（DMP）4300 シリーズ（CSCup92446）
- Cisco Digital Media Player（DMP）4400 シリーズ（CSCup92446）
- Cisco Expressway シリーズ（CSCup25151）
- Cisco Enterprise コンテンツ配信システム（ECDS）（CSCup24139）
- Cisco Hosted Collaboration Mediation 達成（HCM-F）（CSCup24156）
- Cisco インターネット吹流し（CD）（CSCup30939）
- Cisco IP Video Phone E20（CSCup23984）
- Cisco MediaSense（CSCup24113）
- Cisco PowerVu D9190 Conditional Access Manager（PCAM）（CSCup24013）
- Cisco TelePresence Advanced Media Gateway シリーズ（CSCup29733）
- Cisco TelePresence Conductor（CSCup22610）
- Cisco TelePresence Content Server（TCS）（CSCup22349）
- Cisco TelePresence EX シリーズ（CSCup25163）

- Cisco TelePresence Exchange System（CTX）（CSCup23979）
- Cisco TelePresence Integrator C シリーズ（CSCup25163）
- Cisco TelePresence IP Gateway シリーズ（CSCup22636）
- Cisco TelePresence IP VCR シリーズ（CSCup23998）
- Cisco TelePresence ISDN GW 3241（CSCup22632）
- Cisco TelePresence ISDN GW MSE 8321（CSCup22632）
- Cisco TelePresence ISDN Link（CSCup23978）
- Cisco TelePresence MCU すべてのシリーズ（CSCup23994）
- Cisco TelePresence マルチポイント スイッチ（CTMS）（CSCup23980）
- Cisco TelePresence MX シリーズ（CSCup25163）
- Cisco TelePresence MXP シリーズ（CSCup23989）
- Cisco TelePresence Profile シリーズ（CSCup25163）
- Cisco TelePresence Recording Server（CTRS）（CSCup22338）
- Cisco TelePresence Serial Gateway シリーズ（CSCup22633）
- Cisco TelePresence Server 8710、7010（CSCup22629）
- 複数政党制メディア 310 の Cisco TelePresence Server、320（CSCup22629）
- 仮想マシン（CSCup22629）の Cisco TelePresence Server
- Cisco TelePresence スーパバイザ MSE 8050（CSCup22635）
- Cisco TelePresence SX シリーズ（CSCup25163）
- Cisco TelePresence System 1000（CSCup22603）
- Cisco TelePresence System 1100（CSCup22603）
- Cisco TelePresence システム 1300（CSCup22603）
- Cisco TelePresence 1310（CSCup22603）
- Cisco TelePresence System 3000 シリーズ（CSCup22603）
- Cisco TelePresence システム 500-32（CSCup22603）
- Cisco TelePresence システム 500-37（CSCup22603）
- Cisco TelePresence TX9000 シリーズ（CSCup22603）
- Cisco TelePresence T シリーズ（T3）（CSCup25163）
- Cisco TelePresence Video Communication Server（VCS）（CSCup25151）
- Tandberg Codian ISDN GW 3210/3220/3240（CSCup22632）
- Tandberg Codian MSE 8320 モデル（CSCup22632）
- Tandberg 770/880/990 MXP シリーズ（CSCup23989）
- Cisco Video Surveillance 3000 シリーズ IP カメラ（CSCup22372）
- Cisco Video Surveillance 4000 シリーズ IP カメラ（CSCup22381）
- Cisco ビデオ サーベイランス 4300E/4500E 高精細度 IP カメラ（CSCup22377）
- Cisco Video Surveillance 6000 シリーズ IP カメラ（CSCup22372）
- Cisco Video Surveillance 7000 シリーズ IP カメラ（CSCup22372）
- Cisco Video Surveillance PTZ IP カメラ（CSCup22372）
- Cisco Videoscape AnyRes Live（CAL）（CSCup24177）
- Cisco Virtualization Experience Media Engine（CSCup47300）

*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 Unified Contact Center Enterprise のためのおよびホストされる（CSCup24189）
- Cisco Unified Contact Center Express（CSCup34257）のための Cisco Agent Desktop
- Cisco ATA 187 Analog Telephone Adapter（CSCup24458）
- Cisco ATA 190 シリーズ Analog Telephone Adapter（CSCup24100）
- Cisco デスクトップ コラボレーション エクスペリエンス DX650（CSCup22514）
- Cisco Emergency Responder（CER）（CSCup24079）
- Cisco Paging Server（CSCup24093）
- Cisco SPA112 2 ポート電話アダプタ（CSCup24514）
- ルータ内蔵 Cisco SPA122 ATA（CSCup24514）
- Cisco SPA232D Multi-Line DECT ATA（CSCup24514）
- Cisco SPA300 シリーズ IP フォン（CSCup39003）
- Cisco SPA500 シリーズ IP フォン（CSCup39003）
- Cisco SPA510 シリーズ IP フォン（CSCup39003）
- Cisco SPA525 シリーズ IP フォン（CSCup38998）
- Cisco TAPI サービス プロバイダー（TSP）（CSCup35534）
- Cisco コンピュータ テレフォニー インテグレーション オブジェクト サーバ（CTIOS）（CSCup24074）
- Cisco Unified Attendant Console（すべての版）（CSCup23967）
- Cisco Unified Attendant Console Advanced（CSCup24304）
- Cisco Unified Communications 500 シリーズ（CSCup22590）
- Cisco Unified Communications Manager（UCM）（CSCup22670）
- Cisco Unified Communications Manager Session Management Edition（SME）（CSCup22670）
- Cisco Unified Communications Widgets Click to Call（CSCup30489）
- Cisco Unified Contact Center Enterprise（CSCup24074）
- Cisco Unified Contact Center Express（CSCup24073）
- Cisco Unified ドメイン マネージャ（CSCup24018）
- Cisco Unified 6901/6911 の IP フォン（CSCuq05675）
- Cisco Unified 6945 IP Phone（CSCuq05680）
- Cisco Unified 6921/6941/6961 シリーズ IP フォン（CSCup22596）
- Cisco Unified 7800 シリーズ IP フォン（CSCup22531）
- Cisco Unified 7900 シリーズ IP フォン（CSCup22595）
- Cisco Unified 8831 IP Phone（CSCup22638）
- Cisco Unified 8941 IP Phone（CSCup22598）
- Cisco Unified 8945 IP Phone（CSCup22598）
- Cisco Unified 8961 IP Phone（CSCup22539）
- Cisco Unified 9951 IP Phone（CSCup22539）
- Cisco Unified 9971 IP Phone（CSCup22539）
- Cisco Unified IM および存在サービス（CUPS）（CSCup22627）
- Cisco Unified Intelligent Contact Management Enterprise（CSCup24074）

- Cisco Unified IP Conference Phone 8831（CSCup37353）
- Cisco Unified ワイヤレス IP Phone 2920 シリーズ（CSCup37238）
- Cisco Unified Workforce Optimization（CSCup22397）
- Cisco Unity Connection（UC）（CSCup24038）

*ワイヤレス*

- Cisco モビリティ サービス エンジン（MSE）（CSCup22619）
- V3.4.2.x ソフトウェア（CSCup22656）を実行する Cisco Universal Small Cell 5000 シリーズ
- V3.4.2.x ソフトウェア（CSCup22656）を実行する Cisco Universal Small Cell 7000 シリーズ
- Ciscoワイヤレス LAN コントローラ（WLC）（CSCup22587）
- 小さいセル ファクトリ リカバリ ルート ファイルシステム V2.99.4 またはそれ以降（CSCup22656）

**次のシスコ サービスはこの状況報告で文書化されています脆弱性の何れか一つ以上から影響を受けると見つけられました。**

- Cisco USC Invicta シリーズ Autosupport ポータル（CSCup22667）
- Cisco 予防的な Network Operations Center（CSCup24163）
- Cisco Registered Envelope Service（CRES）（CSCup22537）
- Cisco Smart Call Home（CSCup24112）
- Cisco スマートな注意（CSCup24109）
- Cisco WebEx Messenger サービス（CSCup21560）

## 脆弱性を含んでいないことが確認された製品

**注:** 次のリストは顧客がインストールしたオペレーティング システムが付いている顧客提供ホスト（物理サーバーか仮想マシン）でインストールされるように意図されている Ciscoアプリケーションが含まれています。 それらの製品は Cisco製品がインストールされているホスト オペレーティング システムによって Transport Layer Security（TLS）またはデータグラムの転送層セキュリティ（DTLS）機能そのまま使用するかもしれません。 それらのシスコ製品が直接 OpenSSL の影響を受けたバージョンが（従っておよびこの脆弱性によって影響を与えられません）含まれない間、Cisco は顧客がホスト オペレーティング システム インストールを検討し、この脆弱性に対処するのに必要なアップグレードを行うことを推奨しますオペレーティング システム ベンダー 推奨事項および一般のオペレーティング システム セキュリティ上の推奨事項に従って。

**以下のシスコ製品はこの脆弱性から分析され、影響を受けません:**

*Collaboration and Social Media*

- Cisco WebEx Social

*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 IP Communicator
- Cisco NAC Agent for Mac
- Cisco NAC Agent for Web
- Cisco NAC Agent for Windows
- Cisco UC Integration for Microsoft Lync
- Cisco Unified Personal Communicator
- Cisco Unified Video Advantage
- WebEx 生産性ツール

*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 GSS 4400 Series Global Site Selector
- Cisco Application and Content Networking System（ACNS）
- Cisco Extensible Network Controller（XNC）
- Cisco Wide Area Application Services（WAAS）モジュール

*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 Adaptive Security Device Manager
- Cisco Content Security Appliance Updater Servers
- Cisco IronPort Encryption Appliance（IEA）
- Cisco Physical Access Manager

*ネットワーク管理とプロビジョニング*

- Cisco Digital Media Manager（DMM）
- Cisco Discovery サービス
- Cisco Insight Reporter
- Cisco Linear Stream Manager
- Cisco Prime Analytics
- Cisco Prime Cable Provisioning
- Cisco Prime Collaboration 保証マネージャ
- Cisco Prime Home
- Cisco Prime Provisioning for SPs
- Cisco Show and Share（SnS）
- Cisco Unified Intelligence Center
- Cisco Unified Provisioning Manager（CUPM）
- Cisco Wireless Control System（WCS）

- CiscoWorks Network Compliance Manager
- Prime Collaboration プロビジョニング- 10.0

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

- Cisco Broadband Access Center Telco Wireless
- Cisco Nexus 4000 シリーズ

*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 Billing and Measurements Server
- Cisco Finesse
- Cisco MGC ノードは管理します（CMNM）
- Cisco PSTN ゲートウェイ（PGW 2200）
- 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 3900 シリーズ IP フォン
- Cisco Unified Contact Center Domain Manager
- Cisco Unified Contact Center Management Portal
- Cisco Unified Customer Voice Portal（CVP）
- Cisco Unified E-Mail Interaction Manager
- Cisco Unified Operations Manager（CUOM）
- Cisco Unified Service Monitor
- Cisco Unified Sip Proxy
- Cisco Unified Web Interaction Manager
- Cisco Virtual PGW 2200 ソフトスイッチ
- Exony VIM/CCDM/CCMP

*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（CAV）
- Cisco D9034-S Encoder
- Cisco D9054 HDTV Encoder
- Cisco D9804 Multiple Transport Receiver
- Cisco D9824 Advanced Multi Decryption Receiver
- Cisco D9854/D9854-I Advanced Program Receiver
- Cisco D9858 Advanced Receiver Transcoder
- Cisco D9859 Advanced Receiver Transcoder
- Cisco D9865 Satellite Receiver
- Cisco DCM Series 9900-Digital Content Manager
- Cisco TelePresence Management Suite（TMS）

- Cisco TelePresence Management Suite Analytics Extension（TMSAE）
- Cisco TelePresence Management Suite Extension（TMSXE）
- Cisco TelePresence Management Suite Extension for IBM
- Cisco TelePresence Management Suite Provisioning Extension
- Cisco TelePresence Manager（CTSMan）
- Cisco Unified Service Statistics Manager

*シスコ ホステッド サービス*

- Cisco One Portal
- Cisco Services Provisioning Platform（SPP）
- Cisco SmartConnection
- Cisco SmartReports
- Cisco Unified Services Delivery Platform（CUSDP）
- Cisco Universal Small Cell CloudBase
- Cisco WebEx WebOffice および Workspace
- Cisco WebEx メッセンジャーサービス

## 詳細

OpenSSL プロジェクトは 7 脆弱性を 2014 年 6月 5 日表わしました。 これら 1 つ以上の脆弱性は OpenSSL のクライアントとサーバの両方のインストール環境に影響を与えます。 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。

シスコ製品がこれらの脆弱性から受ける影響は、製品ごとに異なります。

シスコ製品については、本ドキュメントの「該当製品」の項に記載されている Cisco Bug ID 情報を参照してください。 追加情報と詳細手順は、製品ごとのシスコ インストレーション ガイド、コンフィギュレーション ガイド、およびメンテナンス ガイドに記載されています。 さらなる説明やアドバイスが必要な場合は、お客様のサポートを担当する組織にお問い合わせください。

## SSL/TLS マン・イン・ザ・ミドル脆弱性

非認証は、影響を受けたクライアント および サーバ間のトラフィックを代行受信する機能のリモート攻撃者 man-in-the-middle攻撃をうまく実行する可能性があります。

この脆弱性は CVE ID CVE-2014-0224 を割り当てられました。

## DTLS 再帰欠陥脆弱性

非認証は、影響を受けたクライアントを攻撃者制御サーバに接続するように確信できるリモート攻撃者 巧妙に細工された DTLS パケット影響を受けたデバイスを送信 する可能性があります。

これは影響を受けたデバイスの部分的か完全な DoS 状態という結果に終る可能性があります。

この脆弱性は CVE ID CVE-2014-0221 を割り当てられました。

## DTLS 無効なフラグメント脆弱性

非認証は設計されている影響を受けたデバイスに、リモート攻撃者 バッファオーバーフロー状態を誘発するように巧妙に細工された DTLS パケットを送る可能性があります。 これは攻撃者が高度な特権の任意のコードを実行する機能を得ることを可能にする可能性があります。

この脆弱性は CVE ID CVE-2014-0195 を割り当てられました。

## SSL_MODE_RELEASE_BUFFERS ヌルポインタ参照解除脆弱性

非認証は、リモート攻撃者 ヌルポインタ参照解除を誘発するように設計されている悪意のある要求を入れる可能性があります。 これは影響を受けたデバイスの部分的か完全な DoS 状態という結果に終る可能性があります。

この脆弱性は CVE ID CVE-2014-0198 を割り当てられました。

## SSL_MODE_RELEASE_BUFFERS セッション インジェクトかサービス拒否の脆弱性

非認証は、リモート攻撃者内容を平行コンテキストにインジェクトするか、または DoS 状態を誘発するように設計されている悪意のある要求を入れる可能性があります。

この脆弱性は CVE ID CVE-2010-5298 を割り当てられました。

## 匿名 ECDH サービス拒否の脆弱性

非認証は、影響を受けたクライアントを攻撃者制御サーバに接続するように確信できるリモート攻撃者 ヌルポインタ参照解除を誘発するように設計されている巧妙に細工された 証明書を入れ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 DoS 状態を発生させることができます。

この脆弱性は CVE ID CVE-2014-3470 を割り当てられました。

## ECDSA NONCE 側チャネル リカバリ不正侵入脆弱性

影響を受けたデバイスのアプリケーションを実行する機能の攻撃者は側チャネル不正侵入によっ

て ECDSA 暗号用具の部分を回復できました。 これは攻撃者がネットワーク通信の保護に使用した暗号化キーを再建することを可能にする可能性があります。

この脆弱性は CVE ID CVE-2014-0076 を割り当てられました。

追加詳細については、顧客は OpenSSL プロジェクト Security Advisory を参照するように勧告されます: http://www.openssl.org/news/secadv_20140605.txt

## 回避策

特定の Cisco製品の可能性のある回避策に関しては、 Ciscoバグ 検索ツールから利用可能な Cisco バグ ID を参照して下さい。

Cisco はこの脆弱性のためのイベント応答を送達しました: http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_OpenSSL_06052014.html

## 修正済みソフトウェア

ソフトウェアアップグレードを検討するとき、顧客は Cisco Security Advisory、応答および表記アーカイブを http://www.cisco.com/go/psirt で参照し、公開および完全なアップグレード ソリューションを判別するためにそれに続く状況報告を検討するように勧告されます。

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が新規リリースで引き続き正しくサポートされていることを十分に確認してください。 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。

## 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。

これらの脆弱性は OpenSSL プロジェクトによって公に 2014 年 6月 5 日表われました。

## 出典

## URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140605-openssl

## 改訂履歴

| | | |
|---|---|---|
| Revision 1.28 | 2015-March-27 | 調査中の製品、脆弱なの、および確認された脆弱ではないセクション アップデートされました。 諮問ステータスは最終に、期待された追加更新移動しませんでした。 |

| | | |
|---|---|---|
| Revision 1.27 | 2015-March-13 | 調査中の製品、脆弱なの、および確認された脆弱ではないセクション アップデートされました。 |
| Revision 1.26 | 2015-February-25 | 影響を受けた Produccts をアップデートし、脆弱なセクションを確認しました。 |
| Revision 1.25 | 2015-January-26 | 該当製品および脆弱性が存在しない製品セクションをアップデートしました。 |
| Revision 1.24 | 2014-November-26 | 該当製品および脆弱性が存在しない製品セクションをアップデートしました。 |
| Revision 1.23 | 2014-November-12 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revision 1.22 | 2014-October-30 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revision 1.21 | 2014-August-06 | 該当製品および脆弱性が存在する製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revision 1.20 | 2014-July-30 | Nexus 2000 年、5000、5600、および 6000 のための追加されたセカンダリ バグ ID CSCup22663。 脆弱性が存在する製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revision 1.19 | 2014-July-23 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revision 1.18 | 2014-July-18 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |

| | | |
|---|---|---|
| Revision 1.17 | 2014-July-14 | 該当製品を、脆弱性が存在する製品アップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revision 1.16 | 2014-July-09 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revision 1.15 | 2014-July-07 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revision 1.14 | 2014-July-03 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revision 1.13 | 2014-June-27 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revision 1.12 | 2014-June-25 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revision 1.11 | 2014-June-23 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revision 1.10 | 2014-June-20 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revision 1.9 | 2014-June-19 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revision 1.8 | 2014-June-18 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revisio | 2014-June- | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップ |

| | | |
|---|---|---|
| n 1.7 | 16 | デートしました。 現在既知該当製品のリンクされたバグID。 |
| Revisio n 1.6 | 2014-June-13 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| Revisio n 1.5 | 2014-June-12 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| リビジョン 1.4 | 2014-June-11 | 該当製品、脆弱性が存在する製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| リビジョン 1.3 | 2014-June-10 | 該当製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 顧客維持されたオペレーティング システムに関する脆弱性が存在しない製品セクションの説明。 |
| リビジョン 1.2 | 2014-June-09 | 該当製品および脆弱性が存在しない製品セクションをアップデートしました。 現在既知該当製品のリンクされたバグID。 |
| リビジョン 1.1 | 2014-June-06 | 該当製品および脆弱性が存在しない製品セクションをアップデートしました。 |
| リビジョン 1.0 | 2014-June-05 | 初回公開リリース |

## 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。