複数のシスコ製品の OpenSSL ハートビート拡張脆弱性

Medium	**アドバイザリーID :** cisco-sa-20140409-heartbleed **初公開日 :** 2014-04-09 03:00 **最終更新日 :** 2014-10-29 16:11 **バージョン 1.26 :** Interim **CVSSスコア :** 5.0 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCuo17488	CVE-2014-0160

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接続されたクライアントかサーバから 64 キロバイトのチャンクのメモリを取得するために非認証を可能にする可能性がある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。

脆弱性は原因抜けた境界チェックインします Transport Layer Security （ TLS ）ハートビート拡張の処理をです。 攻撃者はによって影響を受けたクライアントの脆弱性を不正利用することを試みている場合影響を受けたサーバ設定不正利用する、または悪意のある TLS または DTLS サーバの脆弱性を不正利用することを試みている場合この脆弱性を悪意のある TLS またはデータグラムの転送層セキュリティ（ DTLS ）クライアントの可能性があります。 エクスプロイトは接続されたクライアントかサーバに特に巧妙に細工された TLS または DTLS ハートビート パケットを送る可能性があります。 エクスプロイトは攻撃者が接続されたクライアントからのメモリの限られた部分を表わすことを可能にする可能性がありますまたは各ハートビート パケットのサーバは送信しました。 メモリの表わされた部分はプライベートキーおよびパスワードを含むかもしれない機密情報が含まれている可能性があります。

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 接続を終える SSL サーバとして機能する SSL 接続を開始している SSL クライアントとして機能するデバイスまたはデバイスです。 SSL 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。

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。 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-20140409-heartbleed

該当製品

Cisco は現在どの製品が影響を受けた製品のこの脆弱性および影響から影響を受けるかもしれないか判別するために製品ラインを調査しています。

以下のシスコ製品は現在調査中です:
シスコ製品は現在調査中ではないです。

次のシスコ サービスは現在調査中です:
Cisco ホストされるサービスは現在調査中ではないです。

サブセクションに下記のリストされている製品とサービスに確認されるこの脆弱性への公開がありました。 追加製品はこれらのセクションに調査が続くように追加されます。

脆弱性のある製品

顧客はバグが更新済のとき問題詳細を表示し、自動通知を受信するためにオプションで *電子メール通知*機能を『Save Bug』 を選択 し、アクティブにするように Ciscoバグ 検索ツールを参照できます興味を起こさせました次のバグの何れかの進行状況のトラッキングに。

以下のシスコ製品はこの脆弱性から影響を受けます:

- OpenFlow [CSCuo30098] のための Cisco エージェント
- iOS [CSCuo17488] のための Cisco AnyConnect セキュア モビリティ クライアント
- Cisco ASA CX コンテキストわかっているセキュリティ[CSCuo24523]
- Common Services Platform Collector（ CSPC ） Cisco [CSCuo29151]
- Cisco デスクトップ コラボレーション エクスペリエンス DX650 [CSCuo16892]
- Cisco Edge 340 デジタル メディア プレーヤー[CSCuo24301]
- Cisco Expressway シリーズ[CSCuo16472]
- Cisco FireAMP Private Cloud バーチャル アプライアンス
- Cisco IOS XE [CSCuo19730]
- Cisco Cisco インターネット吹流し CD [CSCuo31566]
- Cisco Jabber Video for TelePresence（ Movi ） [CSCuo28855]
- Cisco 仲間製品[CSCuo22177]
- Cisco モビリティ サービス エンジン（ MSE ） [CSCuo20622]
- Cisco MS200X イーサネット アクセス スイッチ[CSCuo18736]
- Cisco OnePK オールインワン VM [CSCuo19843]
- 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 [CSCuo22921]
- Cisco Prime Collaboration 配備[CSCuo34385]

- Cisco Prime IP Express [CSCuo35657]
- Cisco Prime License Manager [CSCuo32735]
- Cisco Prime Network Registrar（CPNR）[CSCun82386]
- Cisco Prime Network Services Controller [CSCuo20385]
- Cisco Prime Security Manager [CSCuo27123]
- Cisco Security Manager [CSCuo19265]
- Cisco Small Business ISA500 シリーズ統合型セキュリティ アプライアンス[CSCuo29778]
- Cisco TelePresence 1310 [CSCuo20210]
- Cisco TelePresence Conductor [CSCuo20306]
- Cisco TelePresence EX シリーズ[CSCuo26378]
- Cisco TelePresence Integrator C シリーズ[CSCuo26378]
- Cisco TelePresence IP Gateway シリーズ[CSCuo21597]
- Cisco TelePresence ISDN GW 3241 [CSCuo21486]
- Cisco TelePresence ISDN GW MSE 8321 [CSCuo21486]
- Cisco TelePresence ISDN Link [CSCuo26686]
- Cisco TelePresence MX シリーズ[CSCuo26378]
- Cisco TelePresence Profile シリーズ[CSCuo26378]
- Cisco TelePresence Serial Gateway シリーズ[CSCuo21535]
- Cisco TelePresence Server 8710、7010 [CSCuo21468]
- 複数政党制メディア 310 の Cisco TelePresence Server、320 [CSCuo21468]
- 仮想マシン[CSCuo21468] の Cisco TelePresence Server
- Cisco TelePresence System 1000 [CSCuo20210]
- Cisco TelePresence System 1100 [CSCuo20210]
- Cisco TelePresence システム 1300 [CSCuo20210]
- Cisco TelePresence System 3000 シリーズ[CSCuo20210]
- Cisco TelePresence システム 500-32 [CSCuo20210]
- Cisco TelePresence システム 500-37 [CSCuo20210]
- Cisco TelePresence スーパバイザ MSE 8050 [CSCuo21584]
- Cisco TelePresence SX シリーズ[CSCuo26378]
- Cisco TelePresence TX9000 シリーズ[CSCuo20210] バージョン 6.1.2.0 および前に
- Cisco TelePresence Video Communication Server（VCS）[CSCuo16472]
- Cisco Unified 7800 シリーズ IP フォン[CSCuo16987]
- Cisco Unified 8961 IP Phone [CSCuo16938]
- Cisco Unified 9951 IP Phone [CSCuo16938]
- Cisco Unified 9971 IP Phone [CSCuo16938]
- Cisco Unified Communications ドメイン マネージャ（Cisco Unified CDM）10.1(1) [CSCur10784]
- Cisco Unified Communications Manager（UCM）10.0 [CSCuo17440]
- Cisco Unified Communications Manager Session Management Edition（SME）[CSCuo17440]
- Cisco Unified Presence Server（Cisco UPS）[CSCuo21298]、[CSCuo21289]
- Cisco Unified Workforce Optimization [CSCuo43820]

- Cisco Unity Connection （ UC ） [CSCuo30041]
- V3.4.2.x ソフトウェア[CSCuo22301] を実行する Cisco Universal Small Cell 5000 シリーズ
- V3.4.2.x ソフトウェア[CSCuo22301] を実行する Cisco Universal Small Cell 7000 シリーズ
- Cisco Videoscape Conductor [CSCuo46307]
- VDS-IS [CSCuo43012] を流すインターネットのための Cisco ビデオ分配スイート
- Cisco Video Surveillance 3000 シリーズ IP カメラ[CSCuo37282]
- Cisco Video Surveillance 4000 シリーズ IP カメラ[CSCuo37288]
- Cisco ビデオ サーベイランス 4300E/4500E 高精細度 IP カメラ[CSCuo37283]
- Cisco Video Surveillance 6000 シリーズ IP カメラ[CSCuo37282]
- Cisco Video Surveillance 7000 シリーズ IP カメラ[CSCuo37282]
- Cisco Video Surveillance PTZ IP カメラ[CSCuo37282]
- Android [CSCuo20617] のための Cisco WebEx Meetings
- Windows 電話 8 [CSCuo32707] のための Cisco WebEx Meetings
- Cisco WebEx Meetings サーバ（ クライアント ） [CSCuo29780]
- Cisco WebEx Meetings サーバ バージョン 2.x [CSCuo17528]
- Cisco ASR 1000 シリーズ向け Cisco WebEx ノード[CSCuo33614]
- Cisco WebEx Node for MCS [CSCuo33612]
- Cisco Wireless Location Appliance [CSCuo20622]
- 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 [CSCuo22358]
- Tandberg Codian MSE 8320 モデル[CSCuo21486]
- Tandberg Codian ISDN GW 3210/3220/3240 [CSCuo21486]

その他のCisco製品はこの脆弱性から影響を受けるかもしれません。 該当製品のリストは調査として続きますアップデートされます。

脆弱としてリストされている上の製品のそれぞれのために次についての情報は関連する Cisco バグ ID で使用できるようにされます:

- 脆弱で、非脆弱なリリース
- 修正を組み込む最初リリース
- 回避策および軽減（ もし可能であれば ）
- 影響を受けた製品の機能ごとのインパクト・アセスメント

Cisco 次のホストされるサービスはこの脆弱性から影響を受けます:

Cisco ホストされるサービスは現在影響を受けると知られていません。

Cisco 次のホストされるサービスは脆弱として以前に示され、remediated:

- Cisco Registered Envelope Service （ CRES ） [CSCuo16974] [CSCuo17116]
- Cisco USC Invicta シリーズ Autosupport ポータル
- Cisco WebEx メッセンジャーサービス

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 システムの顧客提供ホスト（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（およびそれ故に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、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ために顧客を推奨します。

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:

- Cisco 1000 シリーズ Connected Grid ルータ
- Cisco 200 シリーズ スマートなスイッチ
- Cisco 300 シリーズによって管理されるスイッチ
- Cisco 500 シリーズ スタック可能管理されたスイッチ
- Cisco ACE アプリケーション制御エンジン アプライアンス
- 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、ACE30）
- Cisco ACE グローバルサイトセレクタ アプライアンス（GSS）
- Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Cisco Adaptive Security Device Manager （ASDM）
- Cisco Agent Desktop
- Cisco 異常ガード モジュール
- Cisco AnyConnect Secure Mobility Client for Android
- デスクトップ プラットフォームのための Cisco AnyConnect セキュア モビリティ クライアント
- Cisco Application and Content Networking System（ACNS）ソフトウェア
- Cisco Application Networking Manager （ANM）
- Cisco ASR 5000 シリーズ
- Cisco ATA 187 Analog Telephone Adapter
- Cisco Broadband Access Center Telco Wireless
- Cisco Catalyst 6500 シリーズおよび Cisco 7600 シリーズ Firewall Services Module （FWSM）
- Cisco Catalystオペレーティング システム（CatOS）
- Cisco Computer Telephony Integration Object Server（CTIOS）
- Cisco Configuration Professional
- Cisco Connected Grid Device Manager
- Cisco Connected Grid Network Management System
- Cisco Content Security Management Appliance (SMA)

- Cisco SSL 対応コンテント スイッチング モジュール（CSM-S）
- Cisco CSS 11500 シリーズ コンテンツ サービス スイッチ
- Cisco CVR100W Wireless-N VPN ルータ
- Cisco D9034-S Encoder
- Cisco D9036 Modular Encoding Platform
- 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 シリーズ D9900 デジタル コンテンツ マネージャ
- Cisco Digital Media Manager（DMM）
- Cisco Digital Media Player
- Cisco DPC/EPC 2202 VoIP ケーブルモデム
- Cisco DPC/EPC 2203 VoIP ケーブルモデム
- Cisco DPC/EPC 3208 VoIP ケーブルモデム
- Cisco DPC/EPC2100 ケーブルモデム
- ワイヤレスアクセスポイントが付いている Cisco DPC/EPC2325 住居ゲートウェイ
- 組み込みデジタル音声アダプターが付いている Cisco DPC/EPC2425 ワイヤレス住居ゲートウェイ
- Cisco DPC/EPC2434 VoIP ワイヤレス ホームゲートウェイ
- Cisco DPC/EPC2505 ケーブルモデム
- Cisco DPC/EPC2607 ケーブルモデム
- Cisco DPC/EPC3010 ケーブルモデム
- Cisco DPC/EPC3212 VoIP ケーブルモデム
- Cisco DPC2320 および EPC2320 ワイヤレス住居ゲートウェイ
- Cisco DPC2325R2 および EPC2325R2 ワイヤレス住居ゲートウェイ
- Cisco 組み込みデジタル音声アダプターが付いている DPC2420 および EPC2420 ワイヤレス住居ゲートウェイ
- Cisco DPC3000/EPC3000 ケーブルモデム
- Cisco DPC3008/EPC3008 ケーブルモデム
- Cisco DPC3825 および EPC3825 8x4 DOCSIS 3.0 ワイヤレス住居ゲートウェイ
- Cisco DPC3827 および EPC3827 ワイヤレス住居ゲートウェイ
- Cisco DPC3828 および EPC3828 DOCSIS/EuroDOCSIS 3.0 8x4 ワイヤレス住居ゲートウェイ
- Cisco DPC3925 および EDVA の EPC3925 8x4 DOCSIS 3.0 ワイヤレス住居ゲートウェイ
- Cisco DPC3928 および EPC3928 DOCSIS/EuroDOCSIS 3.0 組み込みデジタル音声アダプターが付いている 8x4 ワイヤレス住居ゲートウェイ
- Cisco DPC3939 DOCSIS 3.0 16x4 ワイヤレス住宅音声ゲートウェイ
- Cisco DPQ/EPQ2160 DOCSIS 2.0 ケーブルモデム

- Cisco DPQ2202 VoIP ケーブルモデム
- デジタル音声アダプターが付いている Cisco DPQ2425 ワイヤレス住居ゲートウェイ
- Cisco DPQ3212 VoIP ケーブルモデム
- EDVA の Cisco DPQ3925 8x4 DOCSIS 3.0 ワイヤレス住居ゲートウェイ
- Cisco DPR/EPR2320、ワイヤレスアクセスポイントが付いている DPR2325 ケーブルモデム
- Cisco DPR362 ケーブルモデムおよびルータ
- Cisco DPX/EPX 2203 VoIP ケーブルモデム
- Cisco DPX/EPX 2203C VoIP ケーブルモデム
- Cisco DPX/EPX2100 ケーブルモデム
- Cisco DPX100/120 ケーブルモデム
- Cisco DPX110 ケーブルモデム
- Cisco DPX130 ケーブルモデム
- Cisco DPX213 VoIP ケーブルモデム
- Cisco DPX2213 VoIP ケーブルモデム
- Cisco Edge 300 Digital Media Player
- Cisco Email Security Appliance (ESA)
- Cisco Emergency Responder（CER）
- Cisco Enterprise Content Delivery System (ECDS)
- Cisco ESW2 シリーズ拡張スイッチ
- Cisco Extensible Network Controller（XNC）
- Cisco Finesse
- Cisco 識別 サービス エンジン（ISE）
- Cisco Insight Reporter
- Cisco Integrated Management Controller（IMC）
- Cisco Intelligent Automation for Cloud
- Cisco IOS XR
- Cisco IOS
- Cisco IP Communicator
- Cisco IP Interoperability and Collaboration System (IPICS)
- Cisco IP Video Phone E20
- Cisco IPS
- Cisco IronPort Encryption Appliance（IEA）
- Cisco Jabber for Android
- Cisco Jabber for iOS
- Cisco Jabber for Mac
- Cisco Jabber for Windows
- Cisco Jabber Software Development Kit
- Cisco Jabber Video for iPad
- Cisco Jabber Voice for Android
- Cisco Jabber Voice for iPhone
- Cisco Linear Stream Manager

- Cisco MDS スイッチ
- Cisco MediaSense
- Cisco Meraki は屋内アクセス ポイントをクラウド管理しました
- Cisco Meraki は屋外アクセス ポイントをクラウド管理しました
- Cisco Meraki MS Access スイッチ
- Cisco Meraki MX セキュリティ アプライアンス モデル
- Cisco Mobile Wireless Transport Manager
- Cisco モデル デジタル音声の DPC2420R2 および EPC2420R2 ワイヤレス住居ゲートウェイ
- Cisco モデル デジタル音声の DPC2425R2 および EPC2425R2 ワイヤレス住居ゲートウェイ
- Cisco Multicast Manager
- Cisco MXE 3500 シリーズ（Media Experience Engines）
- Cisco MXE 5600 シリーズ
- Mac のための Cisco NAC エージェント（Clean Access）
- Web のための Cisco NAC エージェント（Clean Access）
- Windows のための Cisco NAC エージェント（Clean Access）
- Cisco NAC アプライアンス
- Cisco NAC Guest Server
- Cisco NAC Manager
- Cisco NetFlow 世代別 3000 シリーズ機器
- Microsoft Hyper-V 向け Cisco Nexus 1000V スイッチ
- VMware vSphere 向け Cisco Nexus 1000V スイッチ
- Cisco Nexus 1010 Virtual Services Appliance
- Cisco Nexus 1100 バーチャル サービス アプライアンス
- Cisco Nexus 2000 シリーズ Fabric Extender
- Cisco Nexus 3000 Series Switches
- Cisco Nexus 4000 シリーズ スイッチ
- Cisco Nexus 5000 Series Switches
- Cisco Nexus 6000 Series Switches
- Cisco Nexus 7000 Series Switches
- Cisco Nexus 9000 Series Switches
- Cisco ONS 15100 シリーズ
- Cisco ONS 15200 シリーズ DWDM システム
- Cisco ONS 15300 シリーズ
- Cisco ONS 15500 シリーズ
- Cisco ONS 15600 シリーズ
- Cisco ONS 15800 シリーズ DWDM プラットフォーム
- Cisco Packaged Contact Center Enterprise
- Cisco Paging Server
- Cisco Physical Access Gateway
- Cisco Physical Access Manager

- Cisco PowerVu D9190 Conditional Access Manager（PCAM）
- Cisco Prime Access Registrar
- Cisco Prime Analytics
- Cisco Prime Assurance Manager
- Cisco Prime Cable Provisioning
- Cisco Prime Central for SPs
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Manager
- Cisco Prime Collaboration Provisioning
- Cisco Prime Data Center Network Manager（DCNM）
- Cisco Prime Home
- Cisco Prime Infrastructure
- Cisco Prime LAN Management Solution（LMS）
- Cisco Prime Network
- Cisco Prime Network Analysis Module（NAM）アプライアンス（NAM）
- Cisco Prime Optical for SPs
- SPS のための Cisco Prime Performance Manager
- Cisco Prime Provisioning for SPs
- Cisco Quantum Policy Suite (QPS)
- Cisco Quantum SON Suite（Cisco Quantum SON スイート）
- Cisco Quantum 仮想パケットコア
- Cisco Remote Silent Monitoring
- Cisco RV016 VPN Router
- Cisco RV042 VPN Router
- Cisco RV082 VPN Router
- Cisco RV110W ワイヤレスN VPN Router
- Cisco RV120W ワイヤレスN VPN Router
- Cisco RV180 VPN Router
- Cisco RV180W ワイヤレスN VPN Router
- Cisco RV215W Wireless-N VPN ルータ
- Cisco RV220W ワイヤレスN VPN Router
- Cisco RV315W Wireless-N VPN ルータ
- Cisco RV320 VPN Router
- Cisco RV325 VPN Router
- Cisco SCE 8000 シリーズ Service Control Engine
- Cisco SCE 2000 シリーズ サービス コントロール エンジン
- Cisco SCE 1000 シリーズ Service Control Engine
- Cisco Secure Access Control Server（ACS）
- Cisco Service Control Subscriber Manager
- Cisco Service Control Collection Manager
- Cisco Service Control Application for Broadband
- Cisco Show and Share（SnS）

- Cisco SocialMiner
- Cisco Sourcefire アプライアンス（これには 3D 両方システムおよび SSL アプライアンスが含まれています）
- Cisco SSL サービス モジュール（SSLM）
- Cisco TelePresence Advanced Media Gateway Series
- Cisco TelePresence Content Server（TCS）
- Cisco TelePresence Exchange System（CTX）
- Cisco TelePresence IP VCR Series
- Cisco TelePresence Management Suite（TMS）
- Cisco TelePresence Management Suite Analytics Extension
- Cisco TelePresence Management Suite Extension for IBM Lotus Notes
- Cisco TelePresence Management Suite Extension for Microsoft Exchange
- Cisco TelePresence Management Suite Network Integration Extension
- Cisco TelePresence Management Suite Provisioning Extension
- Cisco TelePresence Manager（CTSMan）
- Cisco TelePresence MCU（すべてのシリーズ）
- Cisco TelePresence Multipoint Switch (CTMS)
- Cisco TelePresence MXP シリーズ
- Cisco TelePresence Recording Server（CTRS）
- Cisco トラフィック異常探知器
- Cisco UC Integration IBM Sametime のために
- Cisco UC Integration for Microsoft Lync
- Cisco UC Integration Microsoft Office 伝達者のために
- Cisco UCS B シリーズ（ブレード）サーバ
- Cisco UCS C-Series (Standalone Rack) Servers
- Cisco UCS Central
- Cisco UCS ファブリックは相互接続します
- Cisco UCS Invicta Series Solid State Systems
- Cisco Unified 3900 シリーズ IP フォン
- Cisco Unified 6900 シリーズ IP フォン
- Cisco Unified 7900 シリーズ IP フォン
- Cisco Unified 8941 IP フォン
- Cisco Unified 8945 IP フォン
- Cisco Unified Attendant Console（すべての版）
- Cisco Unified Attendant Console Advanced
- Cisco Unified Client Services Framework
- Cisco Unified Communications 500 シリーズ
- Cisco Unified Communications ドメイン マネージャ（CUCDM）8.1.4 およびそれ以前
- Cisco Unified Communications Manager（UCM）9.1(2) およびそれ以前
- Cisco Unified Communications Widgets Click to Call
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express

- Cisco Unified Customer Voice Portal（CVP）
- Cisco Unified Department Attendant Console
- Cisco Unified E-Mail Interaction Manager（EIM）
- Cisco Unified Enterprise Attendant Console
- Cisco Unified Intelligence Center
- Cisco Unified Intelligent Contact Management Enterprise
- Cisco Unified IP Conference Phone 8831
- Cisco Unified 会合場所 アプリケ– ションサーバおよび Webサーバ
- Cisco Unified Mobility
- Cisco Unified Operations Manager
- Cisco Unified Personal Communicator
- Cisco Unified Provisioning Manager（CUPM）
- Cisco Unified Quick Connect
- Cisco Unified Service Monitor
- Cisco Unified Service Statistics Manager
- Cisco Unified Sip Proxy
- Cisco Unified Video Advantage
- Cisco Unified Web Interaction Manager（WIM）
- Cisco Video Surveillance メディア サーバ ソフトウェア
- Cisco Video Surveillance オペレーション マネージャ ソフトウェア
- Cisco Videoscape AnyRes Live（CAL）
- Cisco Videoscape AnyRes VOD（CAV）
- Cisco Virtual Network Management Center
- Cisco Virtualization Experience Media Engine
- Cisco Virtual Security Gateway for Microsoft Hyper-V
- VMware のための Cisco Virtual Security Gateway
- Cisco VPN Client
- VoIP の Cisco WAG310G ワイヤレスG ADSL2+ ゲートウェイ
- Cisco WAP121 ワイヤレスN アクセス ポイント
- Cisco WAP321 ワイヤレスアクセスポイント
- Cisco WAP4410N ワイヤレスN アクセス ポイント
- Cisco WAP551/561 ワイヤレスN アクセス ポイント
- Cisco Web Security Appliance (WSA)
- Windows のための Cisco WebEx 接続応答 クライアント
- Cisco WebEx Meetings for BlackBerry
- Cisco WebEx Meetings Server versions 1.x
- Cisco WebEx Productivity Tools
- Cisco WebEx Social
- Cisco Wide Area Application Services（WAAS）
- Cisco Wide Area Application Services（WAAS）Express（IOS）
- Cisco Wide Area Application Services（WAAS）モジュール
- Cisco Wireless Control System（WCS）

- Ciscoワイヤレス LAN コントローラ（WLC）
- CiscoWorks Network Compliance Manager
- CiscoWorks Wireless LAN Solution Engine（WLSE）
- Tandberg 770/880/990 MXP シリーズ

Cisco 次のホストされるサービスはこの脆弱性から分析され、影響を受けません:

- Cisco Cloud Web Security
- Cisco Meraki ダッシュボード
- Cisco パートナー サポート サービス
- Cisco Proactive Network Operations Center
- Cisco Smart Call Home
- Cisco Smart Care
- Cisco Smart Net Total Care（SNTC）
- Cisco スマート サービス機能
- Cisco Universal Small Cell CloudBase
- Cisco WebEx Event Center
- Cisco WebEx Meeting Center
- Cisco WebEx Support Center
- Cisco WebEx Training Center
- Cisco WebEx WebOffice

詳細

OpenSSL の Transport Layer Security（TLS）/Datagram Transport Layer Security（DTLS）ハートビート 機能の脆弱性は複数のシスコ製品で非認証、リモート攻撃者を接続されたクライアントかサーバから 64 キロバイトのチャンクのメモリを取得することを許可する可能性があります使用しました。

脆弱性は原因抜けた境界チェックインします TLS ハートビート拡張の処理をです。 攻撃者はによって影響を受けたクライアントの脆弱性を不正利用することを試みている場合影響を受けたサーバ設定不正利用する、または悪意のある TLS または DTLS サーバの脆弱性を不正利用することを試みている場合この脆弱性を悪意のある TLS または DTLS クライアントの可能性があります。攻撃者は接続されたクライアントかサーバにそれから特別細工 された TLS または DTLS ハートビート パケットを送る可能性があります。 エクスプロイトは攻撃者が接続されたクライアントからのメモリの限られた部分を表わすことを可能にする可能性がありますまたは各ハートビート パケットのサーバは送信 しました。 メモリの表わされた部分はプライベートキーおよびパスワードを含むかもしれない機密情報が含まれている可能性があります。

この脆弱性よくある脆弱性および公開（CVE）ID CVE-2014-0160 は割り当てられました

Cisco製品かサービスが脆弱であるかどうか確かめるのに使用される基準がもっぱら TLS/DTLS クライアントかサーバを実装するためにそれが OpenSSL ライブラリの影響を受けたバージョン

に頼るかどうかです。 基準は設定するクライアントかサーバがかもしれないプロトコルのあらゆる特定のセットに分析を制限しません（例えば: HTTPS、SMTP、EAP、等）。
このに基づいて基準は脆弱と同時にこの Security Advisory にであるそのような関係リストされていない製品ベクトルを攻撃者攻撃する Heartbleed を不正利用するのに使用するように試みるかもしれません。

TLS の TLS 層を目標とするのにキューピッド不正侵入は EAP プロトコルを使用して Heartbleed バグをように不正侵入ベクトル不正利用します。 この Security Advisory にリストされている製品は Heartbleed 脆弱性に脆弱のキューピッド不正侵入によってまた変化しないです。

この脆弱性 on Cisco 製品の影響は影響を受けた製品によって変わるかもしれません。

Heartbleed 脆弱性のユニークな特性を与えられる、Cisco は新しいパブリック/プライベートキーペアを作成するために顧客を推奨しインストールして下さいそのキーペアのための新しい証明書を得、ソフトウェア アップデートをインストールした後適切ようにすべての影響を受けた配置で新しい証明書および関連するキーペアを。 これは Cisco およびシスコ 以外のデバイスのために適切な一般のアドバイスです。

シスコ製品に関しては、この文書の Affected Products セクションにリストされている Cisco バグ ID で提供される情報を参照して下さい。 方法に関するその他の情報および詳細な使用説明書はそれらのタスクを行う各製品に Cisco インストール、設定およびメンテナンス ガイドで利用できます。 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。

製品別の情報

Cisco Meraki

Cisco は次に挙げるドキュメントの利用可能なその他の情報を作りました:
https://meraki.cisco.com/blog/2014/04/openssl-and-the-heartbleed-vulnerability/

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

以下の製品は小さいセル ファクトリ リカバリ ルート ファイルシステム V2.99.4 またはそれ以降にてこ入れします。 ファクトリ リカバリ ルート ファイルシステムはフラッシュで保存されないし、Cisco USC CloudBase からダウンロードされ、アクティベーション/リカバリプロセスののためにだけ使用されます。 OpenSSL は自体従って悪意のあるユーザに Cisco あらゆる独自のコードへの公開が呼出されるカール プロセスのメモリスペースがプライベートキーをなかったし、シェル スクリプトから含まれていないカール アプリケーションによって呼出されます、:

- DPH-SO16（Cisco、以前 Ubiquisys）
- FAPE-HSP-5620（OEM）
- FAPO-HSP-5900（OEM）
- FAPR-HSP-5110（OEM）

- FC1020（Cisco、以前 Ubiquisys）
- FC1021（Cisco、以前 Ubiquisys）
- FC1022（Cisco、以前 Ubiquisys）
- FC1060（Cisco、以前 Ubiquisys）
- FC1080（Cisco、以前 Ubiquisys）
- FC170U（Cisco、以前 Ubiquisys）
- FC173U（Cisco、以前 Ubiquisys）
- FC233U（Cisco、以前 Ubiquisys）
- FC235U（Cisco、以前 Ubiquisys）
- FC270U（Cisco、以前 Ubiquisys）
- FEMTO-G3（Cisco、以前 Ubiquisys）
- FEMTOAP-SR1（Cisco、以前 Ubiquisys）
- FEMTOAP-SR2（Cisco、以前 Ubiquisys）
- FMA16301T（OEM）
- FP16201（OEM）
- FP8101（OEM）
- FP8131T（OEM）
- FPA16241T（OEM）
- FPLUS2（Cisco、以前 Ubiquisys）
- G5（Cisco、以前 Ubiquisys）
- G6（Cisco、以前 Ubiquisys）
- S2000（OEM）
- SH170U（Cisco、以前 Ubiquisys）
- SH173U（Cisco、以前 Ubiquisys）
- USC3331（Cisco）
- USC5310（Cisco）
- USC5330（Cisco）
- USC7330（Cisco）
- USC9330（Cisco）
- ZM-000-05-0005（Cisco、以前 Ubiquisys）
- ZP-000-05EU-0004（Cisco、以前 Ubiquisys）
- ZP-000-07EU-0001（Cisco、以前 Ubiquisys）
- ZP-001-03EU-0003（Cisco、以前 Ubiquisys）
- ZP-001-03EU-0005（Cisco、以前 Ubiquisys）
- ZP-001-03EU-0006（Cisco、以前 Ubiquisys）
- ZP-005-02EU-0002（Cisco、以前 Ubiquisys）

Cisco Universal Small Cell 5000 シリーズおよび Cisco Universal Small Cell 7000 シリーズ

悪意のあるユーザはプライベートキーが別途の保護されたメモリスペースで握られると同時にユニバーサル小さいセル（USC）製品のプライベートキーを得ることができません; ただし、悪意のあるユーザは小さいセル内部 O&M データベースおよびコンフィギュレーションの詳細が含ま

れているアクセスメモリにできるかもしれません。

Cisco コラボレーション システム 10.x:

Cisco Unified Communications Manager（UCM）バージョン 10.0、Cisco Unity Connection（UC）バージョン 10.0 および Cisco Unified Presence Server（CUPS）バージョン 10.0 は OpenSSL この アドバイザリに記載される 脆弱性から影響を受けます。 非認証は、影響を受けたポートへの TCP 接続を開く機能のリモート攻撃者脆弱性を不正利用するかもしれません。 不正利用の成功は攻撃者が機密情報を可能性としては表わすことを可能にするかもしれません。

Cisco 音声および存在デバイスはユーザ、管理者、電話および IP 音声ゲートウェイからの接続を許可するためにいくつかのサービス ポートをオープンにします。 SSL か TLS を利用しているこれらのサービスの大半は保護され、攻撃者によって脆弱性を不正利用するためにてこ入れされるかもしれません。

Cisco Unified IP Phone：

セキュア Web管理インターフェイスがイネーブルになっているとき Cisco Unified 7800 シリーズ、Cisco Unified 8961、Cisco Unified 9951、および Cisco Unified IP フォン 9971 脆弱性--にさらされるかもしれません。 さらに、不正侵入はセキュア SIP によって実行され、RTP を保護するかもしれません。

イネーブルにされたとき Web管理インターフェイスに達する機能の非認証、リモート攻撃者、またはそれはデバイスに脆弱性を誘発するかもしれません直接セキュア SIP コールを送信できます。 不正利用の成功は攻撃者が機密情報を可能性としては表わすことを可能にするかもしれません。

Cisco Secure 設定のガイドラインを使用して展開された音声ネットワークは外部攻撃者からの軽減されたリスクにあります。 一般的な使用ネットワークからセグメント化された電話は音声ネットワークにダイレクトアクセスがあるユーザおよび他の電話に不正侵入サーフェイスを制限する必要があります。

Cisco デスクトップ コラボレーション エクスペリエンス:

Cisco デスクトップ コラボレーション エクスペリエンス DX650 デバイスはセキュア Web管理インターフェイスによってイネーブルにされたとき露出されるかもしれません。 OpenSSL システム供給ライブラリを利用するデバイスでインストールされるこれらのデバイスはセキュア SIP、セキュア RTP、また他のどのアプリケーションまたによっても不正利用されるかもしれません。

イネーブルになった場合非認証はデバイスに、Web管理インターフェイスに達する機能のリモート攻撃者直接セキュア SIP コールを送信できますまたは影響を受けたサービスに脆弱性を誘発するかもしれないですアクセスして下さい。 不正利用の成功は攻撃者が機密情報を可能性としては表わすことを可能にするかもしれません。

Cisco Secure 設定のガイドラインを使用して展開された音声ネットワークは外部攻撃者からの軽

減されたリスクにあります。 一般的な使用ネットワークからセグメント化された電話は音声ネットワークにダイレクトアクセスがあるユーザおよび他の電話に不正侵入サーフェイスを制限する必要があります。

ガイドラインを堅くする音声ネットワーク セキュリティ:

Cisco はすべての音声ネットワーク配備に広範囲の設計の指針を提供します。 これにはスプーフィングされたトラフィックが一般的なネットワーク トラフィックからの音声トラフィックの音声ネットワークで、また分離および分離渡られることを防ぐために中間物の推奨される セキュリティ機能設定がおよびエッジ デバイス含まれています。 Cisco コラボレーション システム 10.x のためのセキュリティ情報は次のリンクで利用できます:
http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab10/collab10/security.html

Cisco AnyConnect Secure Mobility Client for iOS

この脆弱性は実行するデバイス iOS 5 またはそれ以前のためにリリースされる Cisco AnyConnect セキュア モビリティ クライアントのバージョンに影響を与えません。

Cisco IOS XE ソフトウェア

Cisco IOS XE ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
2.x.x	脆弱性なし
3.1.xS	脆弱性なし
3.1.xSG	脆弱性なし
3.2.xS	脆弱性なし
3.2xSE	脆弱性なし
3.2.xSG	脆弱性なし
3.2.xXO	脆弱性なし
3.2.xSQ	脆弱性なし
3.3.xS	脆弱性なし
3.3.xSE	脆弱性なし
3.3xSG	脆弱性なし
3.3xXO	脆弱性なし
3.3xSQ	脆弱性なし
3.4.xS	脆弱性なし
3.4.xSG	脆弱性なし
3.5.xS	脆弱性なし
3.5.xE	脆弱性なし
3.6.xS	脆弱性なし
3.6.xE	脆弱性なし
3.7.xS	脆弱性なし
3.8.xS	脆弱性なし
3.9.xS	脆弱性なし

3.10.xS	脆弱性なし
3.11.xS	脆弱
3.12.xS	脆弱
3.12.0aS	脆弱性なし
3.11.2S	脆弱性なし

VMware vSphere 向け Cisco Nexus 1000V スイッチ

製品は脆弱ように最初に報告されました; ただし、追加確認に送達されたリリースがこの問題に脆弱ではないことが確認されました。

回避策

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/ERP-Heartbleed.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。

このセクションは修正済みソフトウェアバージョンについての情報が利用できるとき更新済です。

Cisco AnyConnect Secure Mobility Client for iOS

バージョン 3.0.09353 で固定されるおよび IOSバージョン 6 または 7.を実行するデバイスのための App 記憶装置のダウンロードのために利用可能。

Cisco WebEx Meetings Server

バージョン 2.0MR2 で固定される

Cisco TelePresence Video Communication Server (VCS)

バージョン X7.2.3 および X8.1.1 で固定される

Cisco Expressway Series

バージョン X8.1.1 で固定される

Cisco FireAMP Private Cloud バーチャル アプライアンス
バージョン 1.0.20140409 で固定される

アップデートの後:
ソフトウェア アップデートを完了していた顧客が、後機器の既存の認証を取り替えること更にプライベート クラウド例を保護することを、推奨されます:

自己署名証明書以外証明書を使用している顧客は新しい証明書を手に入れ、インストールする必要があります。 それらの証明書は新しい私用/公開鍵 ペアを使用して生成する必要があります。 顧客は前のパブリック/私用 keypair を再使用するべきではありません。 取り替えられて、メンテナンス モードを出入りしてデバイスを置くことは新しい証明書がロードされるようにします。

デフォルト自己署名証明書を使用している顧客は FireAMP Private Cloud アップデートを行った後次のコマンドの実行によって新しい証明書を生成する必要があります:

```
amp-ctl maintenance enable
amp-ctl regenerate-ssl-certs
amp-ctl maintenance disable
```

これは SSL 証明書を再生し、サービスすべてを再開します。

さらに、顧客は (opadmin および fireamp コンソール) および監査の確認を行うためにログオンします両方のポータルをすべてのパスワードを変える必要があります。 **Cisco Sourcefire**
Cisco Sourcefire 3D アプライアンス (リリースを 4.10.x および 5.x は実行してまで 5.3) および Cisco Sourcefire SSL アプライアンスこの問題に脆弱ではないです。 これらのアプライアンスはこの脆弱性から影響を受けない OpenSSL の 0.9.8 ブランチを実行します。

検出に関するその他の情報に関しては、VRT ブログを参照して下さい。 質問がある場合、Sourcefire テクニカル サポートに連絡して下さい。

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
修正済みソフトウェアはすべての FAPs のための Cisco USC CloudBase に、更新であることの計画のフェーズに現在ある以下の製品を除いて展開されました、: FPLUS2-000X、G5-000X、G6-000X シリーズ、FEMTOAP-SR1-000X および FEMTOAP-SR2-000X。

不正利用事例と公式発表

多重スキャンが試みる、可能性としてはこの アドバイザリに記載される 脆弱性の不正利用の成功広く説明されていますこと Cisco製品のセキュリティ上の問題に対する回答チーム (PSIRT) はわかってい; ただし、Cisco はシスコ製品またはサービスのあらゆる不正利用に気づいていません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed

改訂履歴

Revision 1.26	2014-October-29	フォーマッティング問題を解決しました。
Revision 1.25	2014-October-09	脆弱ように最近リリースされた Cisco Unified Communications ドメイン マネージャ バージョン 10.1(1)をリストしました。
Revision 1.24	2014-June-06	脆弱性が存在する製品をアップデートし、セクションを詳述します。 明示的にキューピッド不正侵入をアドレス指定しました。
Revision 1.23	2014-May-23	詳細セクションをアップデートしました。 ターゲット プラットフォームの初期リリースの前に修正を組み込むことを再製したように脆弱なリストから IOS XE 3.12.0aS バージョンを取除きました。
Revision 1.22	2014-May-22	該当製品を、脆弱性が存在する製品、脆弱性が存在しない製品アップデートし、セクションを詳述します。 脆弱な物のリストに IOS XE 3.12.0aS リリースを追加しました。
Revision 1.21	2014-May-15	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。 より詳しい調査に Cisco Edge 300 デジタル メディア プレーヤーは脆弱性が存在しない製品セクションに移動されました。
Revision 1.20	2014-May-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。 Cisco パートナー サポート サービス サービスは脆弱性が存在しない製品セクションに移動されました。
Revision 1.19	2014-May-06	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。
Revisi	2014-	該当製品、脆弱性が存在する製品、脆弱性が存在しない製品および不正利用事例と公式発

on 1.18	May-02	表セクションをアップデートしました。
Revision 1.17	2014-April-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。
Revision 1.16	2014-April-29	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。
Revision 1.15	2014-April-28	該当製品を、脆弱性が存在する製品、脆弱性が存在しない製品アップデートし、セクションを詳述します。
Revision 1.14	2014-April-25	該当製品、脆弱性が存在する製品、脆弱性が存在しない製品およびソフトウェア バージョン および 修正をアップデートしました。
Revision 1.13	2014-April-24	該当製品、脆弱性が存在する製品、脆弱性が存在しない製品および詳細をアップデートしました。
Revision 1.12	2014-April-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をアップデートしました。 VMware vSphere 向け Cisco Nexus 1000V スイッチは脆弱性が存在しない製品セクションに移動されました。
Revision 1.11	2014-April-22	該当製品、脆弱性が存在する製品、脆弱性が存在しない製品、詳細およびソフトウェア バージョン および 修正セクションをアップデートしました。
Revision 1.10	2014-April-18	該当製品、脆弱性が存在する製品、脆弱性が存在しない製品およびソフトウェア バージョン および 修正セクションをアップデートしました。
Revision 1.9	2014-April-17	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。
Revision	2014-April-	該当製品、脆弱性が存在する製品、脆弱性が存在しない製品、回避策およびソフトウェア バージョン および 修正セクションをアップデ

1.8	16	ートしました。
Revision 1.7	2014-April-15	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。 脆弱としてマークされる Cisco IP Video Phone E20。 Cisco Prime Security Manager はより詳しい調査を必要とします。
Revision 1.6	2014-April-14	該当製品、脆弱性が存在する製品、脆弱性が存在しない製品、回避策およびソフトウェア バージョン および 修正セクションをアップデートしました。 ＡＢＣ順に配列された製品リスト。
Revision 1.5	2014-April-13	該当製品、脆弱性が存在する製品、脆弱性が存在しない製品、詳細およびソフトウェア バージョン および 修正セクションをアップデートしました。
リビジョン 1.4	2014-April-12	該当製品、脆弱性が存在する製品、脆弱性が存在しない製品およびソフトウェア バージョン および 修正セクションをアップデートしました。
リビジョン 1.3	2014-April-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。
リビジョン 1.2	2014-April-10	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。
リビジョン 1.1	2014-April-10	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。
リビジョン 1.0	2014-April-09	初回公開リリース

利用規約

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。