Mudhraルートおよび中間認証局に対する緊急の不信に関するシスコの情報



Advisory ID : cisco-sa-emudhra-info-ScS22A1r
初公開日 : 2026-10-23 16:00
注: : 2026-11-06 20:40
バージョン 1.8 : Interim
回避策 : No workarounds available
Cisco Bug ID :

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

概要

2026年10月17日から10月20日の間に、eMudhraによって管理される認証局を含む重大なセキュリティ侵害が発見されました。

セキュリティ研究者は、2025年4月の鍵生成式(KGC)での前例のない工ラーにより、8つのeMudhra中間証明書の秘密鍵が根本的に破損していることを実証しました。これにより、誰でも数秒以内にこれらの秘密キーをブルートフォース取得できます。詳細については、「eMudhra Intermediate CA Compromise」およびCisco Talosブログの投稿「Compromise eMudhra intermediate certificates」を参照してください。

Splunkの製品とサービスの詳細については、『Splunk製品（2026年10月）でセキュリティが侵害されたeMudhra中間認証局』を参照してください。

重要：製品がこのアドバイザリに記載されていない場合、シスコのレビューによると、その製品はこの脆弱性の影響を受けません。

このアドバイザリは、追加の情報が入手可能になり次第、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-emudhra-info-ScS22A1r

該当製品

シスコでは、これらの脆弱性の影響を受ける製品およびクラウドサービスを判断するために、製品ラインを調査中です。調査の進捗に応じて、シスコはこのアドバイザリを更新し、影響を受け

る製品およびサービスに関する情報を提供します。

調査中の製品

本アドバイザリに記載された脆弱性の影響に関して現在調査中の製品を以下に示します。

重要：製品がこのアドバイザリに記載されていない場合、シスコのレビューによると、その製品はこの脆弱性の影響を受けません。

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
Secure Client（旧称AnyConnect Secure Mobility 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
Software-Defined AVC（SD-AVC）
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 Secure Workload
ネットワーク管理とプロビジョニング
CloudCenter
コラボレーションの監査および評価ツール
CX Cloud Agent
CX Cloud自動障害管理
Evolved Programmable Network Manager（EPNM）
マネージドサービスアクセラレータ(MSX)
オプティカル ネットワーク コントローラ
セキュアマルウェア分析 – クラウド
セキュアマルウェア分析 – プライベートクラウド（アプライアンス）
セキュリティクラウドTA
セキュアなクライアントクラウド管理
XDR
Routing and Switching - Enterprise and Service Provider
クラウドネイティブブロードバンドネットワークゲートウェイ
Cloud Network Controller（旧称：Cloud APIC）
エンタープライズ NFV インフラストラクチャ ソフトウェア（NFVIS）
サービス統合型仮想ルータ（ISRv）
IOS ソフトウェア
vEdgeルータ
ユニファイド コンピューティング

Cloud Services Platform 2100
音声およびユニファイド コミュニケーション デバイス
Unified Communications Managementクラウド
Unified SIP Proxy ソフトウェア
ワイヤレス
Catalyst 9800 シリーズ ワイヤレス コントローラ
Unified Industrial Wirelessソフトウェア
Merakiデバイス
Meraki vMX

脆弱性のある製品

シスコでは、eMudhra Intermediate CA Compromiseの影響を受ける製品を判断するために、製品ラインを調査中です。このセクションは、情報が入手可能になった時点で更新されます。

次の表に、本アドバイザリに記載されたMudhraの侵害の影響を受けるシスコ製品を示します。影響を受ける製品について、シスコは、シスコの修復手順、製品リリースノート、またはリリースされる可能性のある新しいソフトウェアに関する情報を提供します。

重要：製品がこのアドバイザリに記載されていない場合、シスコのレビューによると、その製品はこの脆弱性の影響を受けません。

影響を受ける製品と修復手順

シスコ製品	シスコの修復情報
IOS XE ソフトウェア	Cisco IOS XEおよびGuestShell CA Trust eMudhra信頼ガイド
IOS XEソフトウェアゲストシェル	CSCwx51613
セキュアファイアウォール適応型セキュリティアプライアンス	Cisco Secure Firewall/Firewall Management Center/Adaptive Security Appliance guidance - Mudhraルートおよび中間認証局に対する緊急不信
Packaged Contact Center Enterprise（PCCE）	CSCwx36769
リアルタイム監視ツール(RTMT)	CSCwx45230
Cisco Secure Email and Web Manager	UpdaterによりTrusted Root 2.8に自動的に更新されました。更新が手動で設定されている場合は、cli->updatenowを使用して新しい信頼されたルート2.8を取得します。
Secure Email Gateway	UpdaterによりTrusted Root 2.8に自動的に更新されまし

シスコ製品	シスコの修復情報
	た。更新が手動で設定されている場合は、cli->updatenowを使用して新しい信頼されたルート2.8を取得します。
Secure Firepower Management Center(FMC)ソフトウェア セキュアファイアウォール脅威対策ソフトウェア	Cisco Secure Firewall/Firewall Management Center/Adaptive Security Appliance guidance - Mudhraルートおよび中間認証局に対する緊急不信
Unified Contact Center Enterprise（CCE）	CSCwx36769
Unified Customer Voice Portal（CVP）	標準の自動ルート証明書更新を使用して、信頼できない証明書リストがバックグラウンドで自動的に更新されます。

影響を受ける製品とソフトウェア修正

シスコ製品	目標リリース日
Adaptive Security Device Manager（ASDM）	ASDMアップグレードウィザード：管理者はエンドポイント証明書を追加できます。 11.0.32.1（2027年3月）
ASR 5000シリーズソフトウェア(StarOS)	2026年11月15日
RoomOSソフトウェアを実行するコラボレーションエンドポイント（ボード、デスク、およびルームシリーズ）	RoomOSオンプレミス： 11.41.2.3 26.7.4.3 RoomOSクラウド 2026年10月/現世代用26.10.1 11.41.1以降（前世代）
Cyber Vision	5.6.2（2026年11月）
Duo	クラウドの修復 – 顧客のアクションは不要
Duoアクセスゲートウェイ3.2.0	「Duo Access Gateway 3.2.0 Released 2026-10-21」の手順に従って、3.2.0にアップグレードします。
Duo Agentic認証コネクタ1.0.1	Duo Agentic Identity for agentgatewayの手順を使用して1.0.1にアップグレードしてください。
Duoネットワークゲートウェイ3.4.1	「Duo Network Gateway 3.4.1 Released 2026-10-22」の手順を使用して3.4.1にアップグレードしてください。
Enterprise Chat and Email	2026.04.1（2026年10月30日）

シスコ製品	目標リリース日
Identity Services Engine（ISE）	Identity Services Engine:Mudhraルートおよび中間認証局に対する緊急不信 ISE 3.3P13（2027年4月） ISE 3.4P8（2027年4月） ISE 3.5P5（2026年12月）
ISEパッシブIDコネクタ(ISE-PIC)	Identity Services Engine:Mudhraルートおよび中間認証局に対する緊急不信 ISE 3.3P13（2027年4月） ISE 3.4P8（2027年4月） ISE 3.5P5（2026年12月）
Intersight 仮想アプライアンス	1.1.8-2（2026年11月）
IOS XR ソフトウェア	IOS XRガイダンス – Mudhraルートおよび中間認証局に対する緊急不信 26.4.1（2026年11月30日）
IP 電話 8800 シリーズ	14.4(1)SR5（2027年1月） 14.4(1)ES1（2026年11月13日）
IP Phone 6800、7800、および8800シリーズマルチプラットフォームファームウェア	12-0-8MPP0001（2026年12月）
Meraki ダッシュボード	クラウドの修復が進行中です。お客様のアクションは不要です。
Meraki MVスマートカメラファームウェア	2026年11月18日
Network Services Orchestrator(NSO) – コンテナのみ影響を受ける	お客様は証明書のアップデートを適用できます。 DNFを使用すると、ca証明書を固定されたものにアップグレードできます(2026.2.92_v9.0.319-100.3.el10_2)。これは、証明書がピン留めされていないためです。 6.4.16（2026年12月8日） 6.6.10（2026年11月17日） 6.7.5（2026年11月17日） 6.8（2026年11月19日）
オプティカルサイトマネージャ	6.4.1（2026年11月）
ポリシースイート(CPS)	26.2.0（2026年10月30日）
プロバイダーモビリティ	2026.04.0（2026年11月6日）

シスコ製品	目標リリース日
セキュアアクセス（クラウド）	クラウドの修復 – 顧客のアクションは不要
Security Manager	CSM Image Manager Settings（CSMイメージマネージャの設定）：管理者はエンドポイント証明書を追加できます。 11.0.32.1（2027年3月）
Cisco Secure Network Analytics	7.6.0および7.6.1ロールアップパッチ（2026年11月）
Smart PHY	27.1（2027年3月16日）
スペースコネクタ	2026年11月30日
Telemetry Broker	修復スクリプト（2026年11月15日）
ThousandEyesエンタープライズエージェントアプリケーションホスティングエージェント	5.2.2
ThousandEyesエンタープライズエージェントブラウザボット	Chromiumバージョン156（2026年11月）
ThousandEyesエンタープライズエージェントドッカーエージェント	1.247.3
ThousandEyesエンタープライズエージェントLinuxエージェント	顧客の修復
ThousandEyesエンタープライズエージェント物理アプライアンスエージェント	自動更新：お客様の操作は不要
ThousandEyesエンタープライズエージェント仮想アプライアンスエージェント	自動更新：お客様の操作は不要
ThousandEyesエンタープライズエージェントMerakiエージェント	1.247.3
Ultra Cloud Core：アクセスおよびモビリティ管理機能	2026.04.0（2026年11月）
Ultra Cloud Core：サブスクライバマイクロサービス インフラストラクチャ	2026.04.1（2026年11月）
Ultra Packet Core：ネットワーク・リポジトリ機能	2026年11月15日
Ultra Packet Core：ポリシー制御機能(PCF)	2026年11月7日
Ultra Packet Core：セッション管理	2026年11月15日

シスコ製品	目標リリース日
機能	
Ultra Packet Core – ユーザプレーン機能	2026年11月15日
Webex Calling	Webex MeetingsのMudhraセキュリティアップデートの影響を受ける証明書を確認し、修正します クラウドの修復
Webex Meetings	クラウドの修復が進行中です。お客様のアクションは不要です。

影響を受けた製品はまだ調査中

シスコ製品	
ケーブルデバイス	注意事項
cBR-8 コンバージド ブロードバンド ルータ	
Prime Cable Provisioning	
ネットワークおよびコンテンツ セキュリティ デバイス	注意事項
AI Defense（ハイブリッドオンプレミス導入）	
ハイパーシールド	
セキュアアクセス診断ソフトウェア	
Cisco Secure Web Appliance	
ネットワーク管理とプロビジョニング	注意事項
APICエンタープライズモジュール (APIC-EM)	
Crosswork Activeトポロジ	
Crosswork Change Automation	
Crosswork Data Gateway	
Crosswork Planning	
Crosswork Service Health	
Crosswork Workflow Manager	
Crosswork Zero Touch Provisioning（ZTP）	
メッシュポリシーエンジン	

シスコ製品	
Modeling Labs	
ネットワーク機能仮想化オーケストレータ	
運用に関するインサイトコレクタ	
スマートライセンスユーティリティ(CSLU)	
Smart Software Manager オンプレミス	
MacOS用ThousandEyesエンドポイントエージェント	
Windows用ThousandEyesエンドポイントエージェント	
Unified Contact Center Express（CCX）	
Routing and Switching - Enterprise and Service Provider	注意事項
Application Policy Infrastructure Controller（APIC）	
MDS 9000 シリーズ マルチレイヤ スイッチ	リリース9.4(1) ~ 9.4(5a)が影響を受けます。コードトレイン9.3には影響はありません。
Nexus 3000 シリーズ スイッチ	リリース9.3(9) ~ 9.3(18)が影響を受けます。コードトレイン10.xはトレイン10.1を除き影響を受けます。
ACI モードの Nexus 9000 シリーズ ファブリック スイッチ	コードトレイン15.xと16.xが影響を受けます。
スタンドアロンNX-OSのNexus 9000シリーズスイッチ	リリース9.3(9) ~ 9.3(18)が影響を受けます。コードトレイン10.xはトレイン10.1を除き影響を受けます。
ユニファイド コンピューティング	注意事項
HyperFlex HX Data Platform	
UCS Director	
音声およびユニファイド コミュニケーション デバイス	注意事項
Cloud Connect	
Finesse	
Jabber for Windows	
Jabber Guest	

シスコ製品	
Unified Intelligence Center	
Virtualized Voice Browser（VVB）	15.0(1)コードトレインに影響があります。

脆弱性を含んでいないことが確認された製品

シスコでは、この問題の影響を受ける製品を判断するために、製品ラインを調査中です。このセクションは、情報が入手可能になり次第、更新されます。

シスコは、この問題が以下のシスコ製品には影響を与えないことを確認しました。

ケーブルデバイス
インテリジェントノードソフトウェア（GS7000ノード）
コラボレーションとソーシャルメディア
Webex Contact Center
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
エンドポイント診断ツール
ネットワークおよびコンテンツ セキュリティ デバイス
高度なWebセキュリティレポート
Secure Network Analyticsホスト分類
UTD Snort IPSエンジンソフトウェア
ネットワーク管理とプロビジョニング
Business ダッシュボード
Catalyst Center（旧DNA Center）
Catalyst SD-WANコントローラ
Catalyst SD-WAN Manager
Common Services Platform Collector（CSPC）
Crosswork Network Controller（アクティブトポロジ）
Crossworkネットワークサービスオーケストレータ
Crosswork Optimization Engine
Duo Authentication Proxy
Elastic Services Controller(ESC)
FindIT ネットワーク管理
IoT Field Network Director
ネットワーク構成と変更管理(NCCM)
Nexus Dashboard

Nexus Dashboard Fabric Controller（NDFC）
Nexusダッシュボードインターフェイス
Nexusダッシュボードオーケストレータ
Optical Network Planner
Prime Collaboration Assuranceを使用する
Prime Infrastructure（サポート終了）
Prime Network
Prime Network Registrar
Prime Performance Manager
セキュアエンドポイント – クラウド
セキュアエンドポイント – エンドポイント
セキュアエンドポイント – プライベートクラウド
セキュアなエンドポイント軌道
ThousandEyes Recorder（廃止）
Routing and Switching - Enterprise and Service Provider
APIC OpenStackおよびコンテナプラグイン
Catalyst 1200 および 1300 シリーズ スイッチ
Connected GridルータIOSソフトウェア
IOS XE Catalyst SD-WANソフトウェア
IOS XE IoTルータ
IOS XE公開キーインフラストラクチャ(PKI)
IOxアプリケーションホスティング（Industrial Ethernet 4000シリーズスイッチ）
Nexus 7000 シリーズ スイッチ
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
ユニファイド コンピューティング
Unified Computing System Manager(UCSM)
ACIを使用したOpenStack向けUCS/ファブリックインターコネクト/グループベースポリシープラグイン
UCS Cシリーズラックサーバ – Integrated Management Controller(IMC)およびBIOS
UCS Central Software
UCS EシリーズM3サーバ(UCS-E160S-M3)
UCS Manager ソフトウェア
UCSサーバユーティリティ（Host Upgrade UtilityおよびServer Diagnostic Utility）
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

会議管理(CMM)
会議サーバ(CMS)
Video Surveillance Manager
音声およびユニファイド コミュニケーション デバイス
コンタクトセンターSIPプロキシ(CCCSP)
Emergency Responder
Expressway Selectシリーズ
Expressway シリーズ
Hosted Collaboration Mediationフルフィルメント
Unified Communications Manager (Unified CM)
Unified Communications Manager IM および Presence Service（Unified CM IM&P）
Unified Communications Manager Session Management Edition（Unified CM SME）
Unity Connection
Unity Express
ワイヤレス
Aironet アクセスポイント
AireOS ワイヤレス LAN コントローラ
Aironet 1800Sシリーズネットワークセンサー
Aironet アクティブ センサー
Catalystアクセスポイント
産業用ワイヤレスモニタ
Mobility Services Engine
シスコクラウドホステッドサービス
スペース（クラウドサービス）

重要：製品がこのアドバイザリに記載されていない場合、シスコのレビューによると、その製品はこの脆弱性の影響を受けません。

詳細

影響

これらの脆弱な秘密キーを所有しているユーザは、インターネット上の任意のドメインに対して不正なTLS/HTTPS証明書を発行する可能性があります。侵害された8つの発行側CAには、次のものが含まれます。

- 6 TLS発行CA:ドメイン検証済み(DV)、組織検証済み(OV)、および拡張検証(EV)を対象とし

ます。
- 2コード署名CA:信頼できる送信元から送られてきたように見える悪意のあるソフトウェアの署名を許可します。

2025年5月には、8つの証明書がSectigoのAAA証明書サービスルートによって交差署名されました。このクロスシグ二チャにより、侵害されたキーは、システムがeMudhraルートをネイティブで信頼していない場合でも、世界中のほぼすべてのデバイス、ブラウザ、およびオペレーティングシステムによって信頼されることが保証されます。

この問題は、侵害されたeMudhra中間証明書を信頼するすべてのシスコ製品に影響します。信頼がシスコのTrusted Root Store(TRS)バンドル、組み込み証明書、またはその他のサードパーティの信頼メカニズムによって管理されているかどうかに関係ありません。

回避策

すべての回避策はこのアドバイザリの「脆弱性のある製品」セクションに記載されます。

不正利用事例と公式発表

Cisco Product Security Incident Response Team(PSIRT)は、このアドバイザリに記載された問題について公式発表が入手可能であることを認識しています。

Cisco PSIRTでは、本アドバイザリに記載されている問題の不正利用事例は確認しておりません。

送信元

この問題を報告していただいたeMudhraに感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-emudhra-info-ScS22A1r

改訂履歴

バージョン	説明	セクション	Status	日付
1.8	調査中の製品と影響を受ける製品を更新。	該当製品	暫定	2026年11月6日
1.7	更新された製品が影響を受けます。	該当製品	暫定	2026年11月5日

バージョン	説明	セクション	Status	日付
1.6	更新された製品が影響を受けます。	該当製品	暫定	2026年11月4日
1.5	調査中の製品、影響を受ける製品、影響を受けない製品を更新	調査中の製品、脆弱性が存在する製品、脆弱性を含んでいないことが確認された製品	暫定	2026年10月30日
1.4	調査中の製品、脆弱性が存在する製品、脆弱性が存在しないことが確認された製品を更新。Splunkアドバイザリへのリンクを追加。	概要および該当製品	暫定	2026年10月28日
1.3	調査中の製品、影響を受ける製品、影響を受けない製品を更新	調査中の製品、脆弱性が存在する製品、脆弱性を含んでいないことが確認された製品	暫定	2026年10月27日
1.2	調査中の製品、影響を受ける製品、影響を受けない製品を更新	調査中の製品、脆弱性が存在する製品、脆弱性を含んでいないことが確認された製品	暫定	2026年10月26日
1.1	調査中の製品、影響を受ける製品、影響を受けない製品を更新	調査中の製品、脆弱性が存在する製品、脆弱性を含んでいないことが確認された製品	暫定	2026年10月24日
1.0	初版リリース	—	暫定	2026年10月23日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、マイデバイス（My Devices）ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。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再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

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。 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。

ソフトウェアのアップグレードを検討する際には、関連するシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレード ソリューション一式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。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。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。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、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。本セキュリティアドバイザリの最新版については、シスコ セキュリティ アドバイザリ ページをご覧ください。Cisco Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを評価します。詳細については、シスコのセキュリティ脆弱性ポリシーを参照してください。

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。