Telepresence SUDI証明書チェーンのセキュリティスキャン結果のトラブルシューティング

内容

問題

セキュリティ脆弱性スキャンは、Cisco TelePresenceビデオコーデックエンドポイントのSSL/TLS証明書関連の調査結果にフラグを付けており、特にTCPポート4053、4060、および4062の信頼できない証明書チェーンを報告しています。脆弱性スキャナは、コーデックがACT2 SUDI CA（組織：Cisco）によって発行されたCS-Room証明書と、シスコルートCA 2048で終了する証明書チェーンを提示することを確認します。セキュリティスキャンシステムでは、組織のセキュリティ要件を満たさない信頼できない証明書チェーンとして、このエラーが報告されます。

セキュリティスキャンによって報告される具体的な結果は次のとおりです。

- 自己署名証明書の検出
- 信頼できない証明書チェーン
- ハッシュアルゴリズムに関する弱点
- 証明書の有効期限の警告

環境

- Cisco TelePresenceビデオコーデックエンドポイント
- Webex Deskシリーズデバイスとオンプレミス登録
- ACT2 SUDI(Secure Unique Device Identifier)チップを搭載したエンドポイント
- セキュリティ脆弱性スキャンインフラストラクチャで証明書チェーンの問題にフラグを付ける

- SUDI証明書を提示するTCPポート4053、4060、および4062

解決方法

Cisco TelePresenceエンドポイント上のSUDI証明書は、組み込み型で不変の証明書であり、サポートされている方法では変更、再生成、または削除できません。これらの証明書は、シスコのTrustworthy Technologies実装の一部であり、特定のセキュリティ機能を提供します。

SUDI証明書の動作について

証明書の動作は、ポートおよびシステムの設定によって異なります。

- ポート4053（ペアサービス）:システムにACT2チップが搭載されている場合にSUDI証明書を使用します。カスタム証明書は、ACT2チップを搭載していないシステム（古いエンドポイント）でのみ使用されます。
- ポート4047:お客様が選択した証明書を使用して、タッチパネルとコーデック間の通信を行います。

証明書の場所と詳細

SUDI証明書は、デバイスの証明書ストアにあります。

```
device:~] $ cd /etc/cacerts_sudi
device:/etc/cacerts_sudi] $ ls
0763c37d.0                9426d327.0                mic-cbasrcarsa4k2099.pem
29cf4e89.0                a094437b.0                mic-cmca.pem
36087b08.0                b35c8d6c.0                mic-cmca2.pem
417aa245.0                cmca2.pem                 mic-cmca3.pem
771a09b9.0                crca2048.pem              mic-cmca4.pem
89087fe6.0                crca2099.pem              mic-crcam2.pem
90359431.0                mic-cbarc2099.pem         mic-harsa-ca.pem
```

ACT2 SUDI CA証明書の詳細：

```
CN = ACT2 SUDI CA
O = Cisco
Valid From: Thursday, June 30, 2011 11:26:57 PM
Valid To: Tuesday, May 15, 2029 1:55:42 AM
```

推奨処置

ステップ1:SUDI証明書の目的とセキュリティ実装を確認します。

SUDI証明書は自己署名されませんが、Cisco Manufacturing CAによって署名されます。これは、次のような不変のIDクレデンシャルとして機能します。

- 製品IDとシリアル番号の管理
- 構成、セキュリティ、監査、管理に対して不変のアイデンティティを提供
- Trust Anchorモジュールチップに暗号バインドされる
- クローン作成やスプーフィングを事実上不可能に

ステップ2:セキュリティチームと協力して、SUDI証明書の結果を除外する

SUDI証明書は変更できず、正当なセキュリティ機能を提供しないため、推奨されるアプローチは次のとおりです。

- セキュリティスキャンツールを設定して、影響を受けるサービスのSUDI証明書チェーンの結果を除外する
- シスコの信頼できるテクノロジーの実装に基づいて、例外のビジネス上の正当性を文書化する
- 必要に応じて、お客様が設定可能な証明書を他のポートに集中してセキュリティスキャンを実行

ステップ3:ソフトウェアアップグレードによる証明書の更新

信頼ストアの証明書の更新は、システムを新しいソフトウェアバージョンにアップグレードすると自動的に行われます。これにより、証明書の有効性が長期にわたって維持されます。

重要な制限

SUDI証明書には次の制限が適用されます。

- 変更、再生成、削除はできません
- 証明書が削除され、デバイスが再起動すると、自動再生成が実行されます
- これらのバックエンドサービスに構成可能な証明書を割り当てる方法はありません
- トラストアンカーの実装は不変であるため、証明書の交換は不可能です

原因

セキュリティスキャンの結果は、シスコのSUDI(Secure Unique Device Identifier)証明書の存在によってトリガーされます。この証明書は、Cisco Root CA 2048にチェーンされている組み込み製造証明書です。これらの証明書は、シスコのTrustworthy Technologies実装の一部であり、セキュリティ上の目的で不変であるように設計されています。証明書は、組織固有のCAではなくシスコのルート認証局(CA)で終端されるため、組織のセキュリティスキャンツールで信頼できると認識されません。これはSUDI対応デバイスで想定される動作であり、セキュリティの脆弱性ではなく設計上の特徴を表しています。

関連コンテンツ

- Cisco Trustworthy Technologiesデータシート
- シスコのテクニカルサポートとダウンロード

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。