Cisco Unity Connection ボイス メッセージ ポートの Cisco Unified Communications Manager 認証および暗号化

Cisco Unity Connection システムの脆弱性のポテンシャル ポイントは、Cisco Unity Connection と Cisco Unified Communications Manager の間の Connection です。次のような脅威が発生する可能性があります。

- 中間者攻撃（Cisco Unified CM と Cisco Unity Connection ボイス メッセージ ポートとの間で流れる情報を攻撃者が監視して改変するプロセス）
- ネットワーク トラフィック スニフィング（Cisco Unified CM、Cisco Unity Connection ボイス メッセージ ポート、および Cisco Unified CM で管理される IP Phone 間でやり取りされる電話機同士の会話やシグナリング情報を、攻撃者がソフトウェアを使用してキャプチャするプロセス）
- Cisco Unity Connection ボイス メッセージ ポートと Cisco Unified CM 間のコールシグナリングの変更
- Cisco Unity Connection ボイス メッセージ ポートとエンドポイント（電話機やゲートウェイなど）との間のメディア ストリームの改変
- Cisco Unity Connection ボイス メッセージ ポートの ID 盗用（Cisco Unity Connection 以外のデバイスが Cisco Unified CM に対して Cisco Unity Connection ボイス メッセージ ポートになりすますプロセス）
- Cisco Unified CM サーバの ID 盗用（Cisco Unified CM 以外のサーバが Cisco Unity Connection ボイス メッセージ ポートに対して Cisco Unified CM サーバになりすますプロセス）

Cisco Unified CM のセキュリティ機能

Cisco Unified CM は、上記の脅威に対して、Cisco Unity Connection との Connection をセキュリティで保護できます。Cisco Unity Connection で使用可能な Cisco Unified CM のセキュリティ機能について、表 A-1 で説明します。

表 A-1　Cisco Unity Connection で使用される Cisco Unified CM のセキュリティ機能 （続き）

セキュリティ機能	説明
シグナリング認証	トランスポート層セキュリティ（TLS）プロトコルを使用して、シグナリング パケットが転送中に改ざんされていないことを検証するプロセスです。シグナリング認証は Cisco 証明書信頼リスト（CTL）ファイルの作成に依存します。 **脅威への対処：**この機能は、次の脅威から保護します。 • Cisco Unified CM と Cisco Unity Connection ボイス メッセージ ポートの間の情報フローを改変する中間者攻撃 • コールシグナリングの改変。 • Cisco Unity Connection ボイス メッセージ ポートの ID 盗用 • Cisco Unified CM サーバの ID 盗用。
デバイス認証	デバイスの ID を検証してエンティティが正当なものであることを確認するプロセスです。この処理は、各デバイスが他のデバイスの証明書を受け入れるときに、Cisco Unified CM と Cisco Unity Connection ボイス メッセージ ポートの間で行われます。証明書が受け入れられると、デバイス間に安全な Connection が確立されます。デバイス認証は Cisco 証明書信頼リスト（CTL）ファイルの作成に依存します。 **脅威への対処：**この機能は、次の脅威から保護します。 • Cisco Unified CM と Cisco Unity Connection ボイス メッセージ ポートの間の情報フローを改変する中間者攻撃 • メディア ストリームの改変。 • Cisco Unity Connection ボイス メッセージ ポートの ID 盗用 • Cisco Unified CM サーバの ID 盗用。

セキュリティ機能	説明
シグナリング暗号化	暗号化の方法を使用して、Cisco Unity Connection ボイス メッセージ ポートと Cisco Unified CM の間で送信されるすべての SCCP および SIP シグナリング メッセージの機密を保護するプロセスです。シグナリング暗号化によって、相手に関連する情報、相手が入力した DTMF 番号、通話の状態、メディア暗号キーなどの情報が意図しないアクセスや不正なアクセスから保護されることが保証されます。 **脅威への対処：**この機能は、次の脅威から保護します。 • Cisco Unified CM と Cisco Unity Connection ボイス メッセージ ポートの間の情報フローを監視する中間者攻撃 • Cisco Unified CM と Cisco Unity Connection ボイス メッセージ ポートの間のシグナリング情報フローを監視するネットワーク トラフィック スニフィング
メディアの暗号化	暗号化の手順を使用して、メディアの機密を保持するプロセスです。このプロセスは、IETF RFC 3711 で定義された Secure Real Time Protocol（SRTP）を使用し、目的の受信者だけが Cisco Unity Connection ボイス メッセージ ポートとエンドポイント（電話機やゲートウェイなど）との間のメディア ストリームを変換できます。サポートされているのは、音声ストリームだけです。メディア暗号化には、デバイス用のメディア マスター キー ペアの作成、Cisco Unity Connection とエンドポイントへのキーの配布、さらにはキーの転送中の安全確保が含まれます。 Cisco Unity Connection とエンドポイントは、そのキーを使用してメディア ストリームの暗号化と復号化を行います。 **脅威への対処：**この機能は、次の脅威から保護します。 • Cisco Unified CM と Cisco Unity Connection ボイス メッセージ ポートの間のメディア ストリームを傍受する中間者攻撃 • Cisco Unified CM が管理する Cisco Unified CM、Cisco Unity Connection ボイス メッセージ ポート、および IP Phone の間を流れる電話通話を盗聴するネットワーク トラフィックのスニフィング