Cisco Unified IP Phone Extension Mobilityモニタリングの脆弱性

Medium

アドバイザリーID : Cisco-SA-20071128-CVE-2007-6190

CVE-2007-6190

初公開日 : 2007-11-28 20:50

最終更新日 : 2012-07-14 17:56

バージョン 2.0 : Final

CVSSスコア : 4.0

回避策 : No Workarounds available

Cisco バグ ID :

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

Cisco Unified IP Phoneデバイスには、認証されたリモートの攻撃者が該当デバイスの会話を傍受し、機密情報が漏えいする可能性のある脆弱性が存在します。

この脆弱性は、Extension Mobility機能の安全でない処理に起因します。 認証されたリモートの攻撃者は、該当デバイスが継続的なReal Time Protocol(RTP)ストリームを攻撃者が制御する場所に送信するように設定することで、この脆弱性を不正利用する可能性があります。 この継続的な送信により、攻撃者は該当デバイスの周囲の物理空間で発生している会話をモニタできる可能性があります。

シスコはこの脆弱性をセキュリティ対策として確認していますが、アップデートは提供されていません。

この脆弱性を不正利用するには、攻撃者は該当デバイスへの認証を許可するのに十分なExtension Mobilityクレデンシャルを所有している必要があります。 攻撃に対して脆弱なのは、組み込みWebサービスとともにExtension Mobility機能が有効になっているデバイスだけです。 さらに、攻撃者は、ユーザがログインしていないエクステンションモビリティ対応の電話機のみを攻撃できます。 エクスプロイトに成功すると、攻撃者はデバイスで進行中の会話を傍受できる可能性があります。

影響を受けるデバイスが不正利用されると、電話機に不具合を示す視覚的な兆候が現れます。 エクスプロイトされたデバイスはスピーカーフォンボタンを点灯させ、LCDディスプレイを搭載し

たデバイスはオフフックを示します。 これらの要因に加えて、VoIPネットワークまたはVLANへのアクセスを必要とする攻撃者は、攻撃の可能性を大幅に低下させます。

該当製品

シスコは次のリンクでセキュリティアドバイザリをリリースしています。cisco-sr-20071128-phone

脆弱性のある製品

Cisco Unified IP Phoneデバイスには脆弱性が存在します。

脆弱性を含んでいないことが確認された製品

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

回避策

アップデートが利用可能になった時点で適用することを推奨します。

音声ネットワークを設定する際には、VoIPテレフォニーのベストプラクティスに従うことをお勧めします。

管理者は、すべてのVoIPトラフィックに専用のVLANを使用することを推奨します。

影響を受けるデバイスには802.11x認証を適用することを推奨します。

ACLを使用して、該当するデバイスのWebサーバへのアクセスを制限することを推奨します。

管理者は、不正アクセスを防止するために、アクセスレイヤスイッチポートにMACアドレスをハード設定することを検討できます。

管理者は、影響を受けるデバイスの組み込みWebサービスを無効にすることを検討できます。

管理者は、Extension Mobility機能を無効にすることを検討できます。

管理者は、影響を受けるデバイスでスピーカフォンおよびヘッドセットの機能を無効にすることを検討できます。

修正済みソフトウェア

契約が有効なシスコのお客様は、CiscoのSoftware Centerからアップデートを入手できます。契約をご利用でないお客様は、1-800-553-2447または1-408-526-7209のCisco Technical Assistance Center(TAC)に連絡するか、tac@cisco.comのEメールでアップグレードを入手できます。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20071128-CVE-2007-6190

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース	適用外	Final	2007年11月28日

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。

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。