Cisco IP Phone SIP はメッセージ サービス拒否の脆弱性を誘います

Medium	**アドバイザリーID :** Cisco-SA-20070320-CVE-2007-1542 **初公開日 :** 2007-03-20 16:35 **最終更新日 :** 2012-07-14 21:01 **バージョン 2.0 :** Final **CVSSスコア :** 3.3 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2007-1542

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

ファームウェアのバージョン 7.4 との Cisco 7940 によりおよび 7960 IP 電話は非認証を可能にする可能性があるサービス拒否（DoS）状態を引き起こすために脆弱性がリモート攻撃者含まれています。

形式が間違った SIP の処理内のエラーによる脆弱性存在はメッセージを誘います。 攻撃者は巧妙に細工されたの送信によってデバイスに誘いますそれは一時 DoS 状態に終って、リブートしますメッセージによりこの脆弱性を不正利用する可能性があります。

Proof-of-concept コードは利用できます。

Cisco はこの脆弱性を確認し、それを訂正するために更新をリリースしました。

この脆弱性を不正利用するために、攻撃者はデバイスが常駐するネットワークにアクセスできなければなりません。 もう一つの不正侵入ベクトルは影響を受けたデバイスに誘うメッセージを悪意のある SIP を渡す可能性がある SIP ゲートウェイです。 通常 IP 電話はネットワーク外部攻撃者はこの脆弱性を不正利用することを防ぐ可能性がある自分自身で常駐します。 ただし、IP Phone への物理アクセスを用いる攻撃者は可能性としては電話のプラグを抜く可能性があり、電話ネットワークに直接その接続からアクセスするために IP Phone は普通にプラグインします。

Cisco はこの脆弱性からファームウェアのバージョン 8.6 を影響を受けませんリリースしました

該当製品

Cisco は次のリンクでセキュリティ応答をリリースしました: cisco-sr-20070320

脆弱性のある製品

ファームウェアのバージョン 7.4 を実行する Cisco 7940 および 7960 IP 電話は脆弱です。

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

管理者は適切な更新を加えるように助言されます。

管理者は分離ネットワークか VLAN に Cisco すべての IP 電話を置くように助言されます。 これは外部攻撃者がこのセキュリティ上の問題を不正利用できることを防ぐのを助けます。

管理者は IP Phone ポートの物理的セキュリティを維持するように助言されます。 必要とされてまでどの未使用ポートでも無効であるはずです。

修正済みソフトウェア

アクティブな契約を持つ Cisco カスタマは次のリンクで Software Center を通して更新を入手できます: Cisco。 契約のない Cisco カスタマは 1-800-553-2447 か 1-408-526-7209 でまたは tac@cisco.com で E メールで Cisco Technical Assistance Center にコンタクトをとってアップグレードを入手できます。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20070320-CVE-2007-1542

改訂履歴

Version	Description	Section	Status	日付

1.0	初版リリース	該当なし	Final	2007-Mar-20

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。