Cisco Unified CallManagerおよび Unified Presence ServerのICMPエコー要求処理におけるDoS脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20070328-CVE-2007-1834 **初公開日 :** 2007-03-28 17:12 **最終更新日 :** 2015-11-25 16:44 **バージョン 1.1 :** Final **CVSSスコア :** 3.3 **回避策 :** Yes **Cisco バグ ID :**	CVE-2007-1834

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 CallManagerおよびUnified Presence Serverには、認証されていないリモートの攻撃者がサービス妨害(DoS)状態を引き起こす可能性のある脆弱性が存在します。

この脆弱性は、大量のICMPエコー要求の不適切な処理に起因します。 攻撃者は、大量のICMPエコー要求をCallManagerまたはPresence Serverシステムに送信することで、この脆弱性を不正利用する可能性があります。 これらの要求により、さまざまなサービスがクラッシュし、その結果DoS状態が発生し、音声サービスに影響を与える可能性があります。

シスコは、セキュリティアドバイザリでこの脆弱性を確認し、アップデートをリリースしました。

Cisco Unified CallManagerはCisco IPテレフォニーソリューションのコール処理コンポーネントで、Unified Presence Serverはテレフォニーソリューションの ID追跡コンポーネントです。 この脆弱性は、これらのコンポーネントがICMPエコー要求を処理する方法に存在します。 該当システムに大量のICMPエコー要求を送信することで、攻撃者はこの脆弱性を不正利用してシステムをクラッシュさせ、音声サービスの中断を引き起こす可能性があります。 この脆弱性は、スプーフィング攻撃によって不正利用される可能性もあります。

このタイプの攻撃（主に総当たり攻撃）を実行するためにエクスプロイトコードは必要ありません。 攻撃の試みを支援し、ping要求でネットワークと特定のデバイスをフラッディングできる多くのネットワークユーティリティソフトウェアパッケージがあります。 これらのユーティリティ

は商用またはオープンソースで、ダウンロードした人が誰でも利用できます。

該当製品

シスコは、Cisco Bug ID CSCsg60930およびCSCsf12698のセキュリティアドバイザリを次のリンクでリリースしました。cisco-sa-20070328-voip

脆弱性のある製品

次のシスコ製品に脆弱性が存在します。

- 5.0(4a)SU1 よりも前の Cisco Unified CallManager 5.0 バージョン
- 1.0(3) よりも前の Cisco Presence Server 1.0 バージョン

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

適切なアップデートを適用することを推奨します。

管理者はICMPエコー要求のブロックを検討できますが、これはネットワーク管理アプリケーションとトラブルシューティング手順に影響を与えます。

IPテレフォニーシステムを絶縁されたネットワーク上に配置し、このネットワークを物理的に保護することを推奨します。

Cisco Applied Intelligenceチームは、更新されたソフトウェアを適用する前に、この脆弱性を悪用しようとする試みを識別して緩和する方法について管理者をガイドする次の関連ドキュメントを作成しました。Identifying and Mitigating Exploitation of Multiple Cisco Unified CallManager and Presence Server Vulnerabilities

修正済みソフトウェア

有効な契約を結んでいるシスコのお客様は、CiscoのSoftware Centerからアップデートを入手できます。契約を結んでいないシスコのお客様は、Cisco Technical Assistance Center(TAC)に1-800-553-2447または1-408-526-7209で連絡するか、tac@cisco.comに電子メールで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）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-20070328-CVE-2007-1834

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	関連リソースへのリンクを更新	複数	Final	2015年11月25日
1.0	初版リリース	適用外	Final	2007 年 3 月 28 日

利用規約

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。