

Cisco Unity Connection 枯渇サービス拒否の脆弱性

Medium	アドバイザーID : Cisco-SA-20081009-CVE-2008-4544	CVE-2008-4544
	初公開日 : 2008-10-09 13:53	
	バージョン 1.0 : Final	
	CVSSスコア : 5.0	
	回避策 : Yes	
	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 Unity により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。^

ネットワークメッセージの不適当な処理によるこの脆弱性存在。^ 非認証、影響を受けたシステムに正規のユーザアクセスを拒否するかもしれない Cisco Unity サーバを利用できないするのにこの脆弱性を不正利用するリモート攻撃者。

Cisco はこの脆弱性を確認しましたが、更新済ソフトウェアは利用できません。

攻撃者は信頼されるに影響を受けたシステムに接続するために内部ネットワークアクセスを必要とするかもしれません。^ はエクスプロイト影響を受けたシステムのそれ以上の接続の確立を防ぐ可能性があります。^ はこのサービス拒否状態ユーザが Cisco Unity サーバにアクセスすることを防ぐ可能性があります。

該当製品

修正済みソフトウェア

次の Cisco Unity バージョンは脆弱です:

Cisco Unity^ 4.2(1) および前

Cisco Unity 5.0(1) および前

Cisco Unity 7.0(2) および前

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。

改訂履歴

バージョン	説明	Section	ステータス	日付
1.0	初版リリース	該当なし	Final	2008-Oct-09

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。本アドバイザリに関する情報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、単独の転載や意識を施した場合、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。