

サービス拒否の脆弱性を処理する Cisco IOS リアルタイムトランスポートプロトコル パッケージ

Medium	アドバイザーID : Cisco-SA-20110610-CVE-2011-1631	CVE-2011-1631
	初公開日 : 2011-06-10 22:07	
	バージョン 1.0 : Final	
	CVSSスコア : 4.3	
	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 IOSソフトウェアにより非認証を可能にする可能性がある目標とされたデバイスのサービス拒否 (DoS) 条件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。

脆弱性は不正なパケットの処理のエラーが原因です。非認証はデバイスへ悪意のあるネットワークパケットを送信することによって、リモート攻撃者脆弱性を不正利用する可能性があります。成功すれば、攻撃者によりデバイスのコンポーネントは DoS 状態に終って、応答することを止めます可能性があります。

Cisco は Security Advisory のこの脆弱性を確認し、更新済ソフトウェアをリリースしました。

Gambino DSP コンポーネントを使用するデバイスだけ脆弱です。異なる DSP コンポーネントが付いているデバイス、か、変化しないですコンポーネントなしのデバイスは。

脆弱性を不正利用するために、攻撃者は影響を受けたデバイスに悪意のあるネットワーク要求を送信する必要があります。攻撃者は内部ネットワークにアクセスが不正利用のための可能性を制限するデバイスに RTP 要求を送信するように要求するかもしれません。

Cisco は CVSS スコアを通してその機能エクスプロイトコード存在を示します; ただし、コードは共用利用可能であると知られていません。

該当製品

修正済みソフトウェア

9.4.14 前に DSPware ファームウェアのバージョンが含まれている 12.4(15)Tx 以前の Cisco IOS ソフトウェア バージョンは影響を受けています。脆弱性が含まれていない Cisco IOS ソフトウェアのより多くの最近のバージョンは DSP ファームウェアのバージョン 10 およびそれ以降を使用します。

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。

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	2011-Jun-10

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。