Cisco IOSÂ VTPÂ 不正 な VersionÂ サービス拒否の脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20060913-CVE-2006-4774 **初公開日 :** 2006-09-13 20:38 **バージョン 1.0 :** Final **CVSSスコア :** 3.3 **回避策 :** Yes **Cisco バグ ID :**	CVE-2006-4774

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 により非認証を可能にする可能性がある VLAN Trunking Protocol （ VTP ）でサービス拒否 （ 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。

Cisco IOSソフトウェアの複数のバージョンの VTP 機能がきちんとローカルネットワークから送信される不正 なパケットを処理しないので存在 する脆弱性。 ローカルネットワーク セグメントに常駐する攻撃者により巧妙に細工されたサマリ パケットによって DoS 状態を引き起こすのにこの脆弱性を不正利用する可能性があります。

Cisco はそれを訂正するために 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。

この脆弱性を不正利用するために、攻撃者はローカルネットワーク セグメントに常駐し、VTP をサポートするデバイスに巧妙に細工されたサマリ パケットを送信 する必要があります。 デバイスは VTP のための*クライアント*か *サーバ*で設定する必要があります。 さらに、パケットはトランク 使用可能なポートで受信する必要があります。 VTP ドメイン パスワードで設定されるスイッチはまだ影響を受けます。

パケットを受信するスイッチはソフトウェア リセット前にプロセス VLAN マネージャの**ウォッチドッグ タイムアウト**または **CPU Hog** のための syslog メッセージを生成します。 不正利用により DoS 状態をまでだけデバイス リブート引き起こします。 繰り返された不正侵入により拡張 DoS 状態を引き起こす可能性があります。

該当製品

修正済みソフトウェア

サーバか クライアントとして VTP 動作モードを持っている Cisco IOSデバイスは脆弱です。

影響を受けた IOS 製品の完全なリストは次のリンクで登録ユーザ向けに利用可能です: (『 Cisco

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	2006-Sep-13

利用規約