

# Cisco IOS VTP 不正な Version サービス拒否の脆弱性

<b>Medium</b>	アドバイザリーID : Cisco-SA-20060913-CVE-2006-4774	<a href="#">CVE-2006-4774</a>
<b>m</b>	初公開日 : 2006-09-13 20:38	<a href="#">4774</a>
	バージョン 1.0 : Final	
	CVSSスコア : <a href="#">3.3</a>	
	回避策 : <a href="#">Yes</a>	
	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 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が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

サーバが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	<a href="#">初版リリース</a>	該当なし	Final	2006-Sep-13

## 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。