Cisco IOS VTP VLAN バッファオーバーフローの脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20060913-CVE-2006-4776 **初公開日 :** 2006-09-13 19:34 **バージョン 1.0 :** Final **CVSSスコア :** 6.0 **回避策 :** Yes **Cisco バグ ID :**	CVE-2006-4776

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 は認証される可能にする可能性がある任意 の コードを実行するために脆弱性がリモート攻撃者含まれています。

Cisco IOS.Â の VTP 機能によって不適当な入力の検証による脆弱性存在は影響を受けたシステムに悪意のある VTP サマリー アドバタイズメントを入れることによって認証されて、リモート攻撃者この脆弱性を不正利用する可能性があります。Â はバッファオーバーフローか、影響を受けたシステムをリセットするか、または攻撃者が任意 の コードを実行するようにすることという結果にこの操作終る可能性があります。

Cisco はセキュリティ応答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、攻撃者はターゲット システムのドメインと一致するドメインを規定 する VTP サマリー アドバタイズメント パケットを細工できる必要があります。Â はこのナレッジ外部攻撃者が判別しことができるようににくくないですかもしれません。その上に Â は、攻撃者 トランク 使用可能なポートのターゲット システムで着くようにパケットを送信 する必要があります。これをする Â は攻撃者 脆弱 な ターゲットのための適切な宛先アドレスを確認する必要があります。トランク 使用可能なポートのターゲット システムに達するローカルネットワーク ネットワーク構成による Â は攻撃者が攻撃を上演できるシステムを制限するかもしれません。

規格によって提案される推奨事項が VTP ドメイン パスワードを設定 することであるので攻撃者はまたこの脆弱性を不正利用するためにこのパスワードを知るか、または推測する必要がありま

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: CSCsd34855 および CSCei54611

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