AVS TCP リレー脆弱性

severity	**アドバイザリーID :** cisco-sa-20060510-avs **初公開日 :** 2006-05-10 16:00 **バージョン 1.0 :** Final **回避策 :** Yes **Cisco バグ ID :**	CVE-2006-2322

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 Application Velocity System （ AVS ）のデフォルト 設定は受信 TCP サービスが HTTP POST メソッド メッセージで組み込まれる要求を処理できる場合あらゆる到達可能な宛先 TCPポートへの TCP 接続の透過的なリレーを可能にします。 この問題はソフトウェアアップグレードを必要としないし、すべての影響を受けた顧客向けの設定コマンドによって軽減することができます。

AVS ソフトウェアの修正済み バージョンはセキュア デフォルト 設定を提供するために修正されました。

Cisco は新しい AVS デバイスをインストールしている影響を受けた顧客向けのこの脆弱性に対処するためにフリーソフトを使用できるようにしました。 利用可能 な回避策はソフトウェアの修正済み バージョンにアップグレードする AVS デバイスを存在 するためのこの脆弱性の影響を軽減するために手動で設定する必要があっても。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060510-avs で掲示されます

該当製品

修正済みソフトウェア

5.0.1 前にすべてのソフトウェア バージョンを稼動する AVS 3110 および 3120 Application Velocity System （ AVS ）は影響を受けています。

- AVS 3110 4.0 および 5.0

- AVS 3120 5.0.0

両方のデバイスのためのすべての以前のバージョンと同様。

脆弱性を含んでいないことが確認された製品

AVS 3180 管理ステーションはこの脆弱性から影響を受けません。

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

リビジョン 1.0	2006-May-10	初版リリース

利用規約