非 DOCSIS プラットフォームで有効に なる DOCSIS 読み書きコミュニティストリング

Medium	**アドバイザリーID :** cisco-sa-20060920-docsis **初公開日 :** 2006-09-20 16:00 **バージョン 1.1 :** Final **CVSSスコア :** 6.0 **回避策 :** Yes **Cisco バグ ID :** CSCsb04965 , CSCsb06658	CVE-2006-4950

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 IAD2400 シリーズ、1900 シリーズ モバイル ワイヤレス エッジルータおよび Cisco VG224 アナログ式電話 ゲートウェイで動作する Cisco IOS Â® ある特定のソフトウェア リリース トレインで存在 する脆弱性。 脆弱なバージョンは SNMP がデバイスで有効に なるときデフォルトによってハードコードされる簡易ネットワーク管理プロトコル（SNMP）コミュニティ ストリングを示すかもしれません。 デフォルト コミュニティ ストリングはサポート Data Over Cable Service Interface Specification （DOCSIS）対応インターフェイスとして不注意にこれらのデバイスを識別した結果です。 このエラーの結果は追加読み書きコミュニティストリングが有効に なるかもしれないことで、デバイスが SNMP 管理のために設定されれば知識がある攻撃者にデバイスに特権アクセスを得る可能性を与えます。

Cisco は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ています。 この脆弱性に対しては、影響を緩和するための回避策があります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060920-docsis で掲示されます。

該当製品

修正済みソフトウェア

該当する Cisco IOS ソフトウェア リリースと動作するかもしれない Ciscoデバイスは下記のものを含んでいます:

- Cisco IAD2430 統合アクセス デバイス
- Cisco IAD2431 統合 アクセス デバイス
- Cisco IAD2432 統合 アクセス デバイス
- Cisco VG224 Analog phone gateway
- Cisco MWR 1900 Mobile Wireless Edge ルータ
- Cisco MWR 1941 モバイル ワイヤレス エッジルータ

脆弱性を含んでいないことが確認された製品

脆弱性を含んでいない製品は次のとおりです。

- Cisco IAD2420 統合 アクセス デバイス
- Cisco IAD2421 統合 アクセス デバイス
- Cisco IAD2423 統合 アクセス デバイス
- Cisco IAD2424 統合 アクセス デバイス

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-September-20	初回公開リリース

利用規約