

Cisco Small Business ビデオ サーベイランス カメラおよび Cisco 4 ポート ギガビット セキュリティ ルータ 認証 バイパス の 脆弱性

Critical アドバイザリーID : cisco-sa-20100421-vsc [CVE-2010-0593](#)
初公開日 : 2010-04-21 16:00
バージョン 1.1 : Final
CVSSスコア : [9.0](#)
回避策 : [Yes](#)
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 Small Business ビデオ サーベイランス カメラおよび Cisco RVS4000 4 ポート ギガビット セキュリティ ルータは認証済みユーザの許可のレベルに関係なく認証済みユーザが他のユーザ向けのパスワードを表示することを可能にする可能性がある脆弱性が含まれています。

権限のないユーザはデバイスの完全な管理アクセスを得るか、または他のユーザの資格情報を表示するのにこの脆弱性を利用する可能性があります。

シスコはこの脆弱性に対処するソフトウェア アップデートをリリースしました。この脆弱性を軽減する回避策はいくつかのデバイスで利用できます。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100421-vsc> で掲示されます。

該当製品

修正済みソフトウェア

この脆弱性は Cisco PVC300 パン傾きオプティカルズーム カメラを除いて Cisco RVS4000 4 ポート ギガビット セキュリティ ルータおよびすべての Cisco Small Business ビデオ サーベイランス カメラに、影響を与えます。これらのカメラは影響を受けています:

- Cisco PVC2300 ビジネス インターネット ビデオ カメラ-オーディオ/PoE

- Cisco WVC200 ワイヤレスG PTZ インターネット ビデオ カメラ-オーディオ
- Cisco WVC210 ワイヤレスG PTZ インターネット ビデオ カメラ-双方向オーディオ
- Cisco WVC2300 ワイヤレスG ビジネス インターネット ビデオ カメラ-オーディオ

脆弱性を含んでいないことが確認された製品

Cisco PVC300 パン傾きオプティカルズーム カメラおよび Cisco スモール ビジネス カメラはこの脆弱性から影響を受けません。

Cisco 他のカメラが製品は現在この脆弱性から影響を受けるために知られていません。

改訂履歴

リビジョン 1.1	2010- May- 17	WVC200 および WVC210 のためのソフトウェア テーブルの更新済最初修正済み バージョン。「また不正利用事例と公式発表」セクションへの追加されたコンテンツ。
リビジョン 1.0	2010- April- 21	初回公開リリース

利用規約

本アドバイザー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。本アドバイザーの情報およびリンクの使用に関する責任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。

本アドバイザー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。