Cisco Router Web Setup は不確かなデフォルト IOSコンフィギュレーションと出荷します

severity	**アドバイザリーID :** cisco-sa-20060712-crws	CVE-2006-3595
	初公開日 : 2006-07-12 16:00	
	バージョン 1.1 : Final	
	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

デフォルト Cisco IOSコンフィギュレーションは Cisco Router Web Setup （ CRWS ）アプリケーションと Cisco IOS HTTP （ Hypertext Transfer Protocol （ HTTP ） ）サーバ Webインターフェイスを通して特権レベル 15 で認証クレデンシャルを必要としないで許可しますコマンドの実行を提供された。 特権レベル 15 は最も高い特権レベル on Cisco IOSÂ® デバイスです。

CRWS アプリケーションの修正済み バージョンは Cisco によって Cisco IOS HTTP サーバ Webインターフェイスに関してセキュア デフォルト IOSコンフィギュレーションおよび追加機能を提供するために修正されました。

この問題は Cisco IOS ソフトウェア アップグレードか CRWS ソフトウェアアップグレードを必要としません。 CRWS の修正済み バージョンにアップグレードすることにし、新しいデフォルト IOSコンフィギュレーションを展開する顧客は推奨される 回避策を展開する必要はありません。 固定 CRWS バージョンにアップグレードしないために選ぶ固定 CRWS バージョンにアップグレードしている現在のコンフィギュレーションを保存する顧客または顧客はこのアドバイザリで識別される回避策を設定する必要があります。

CRWS アプリケーションと提供された新しいデフォルト IOSコンフィギュレーションのその他の情報はこのアドバイザリの詳細 セクションで利用できます。

このアドバイザリは 712-crws で掲示されます。

該当製品

修正済みソフトウェア

コンフィギュレーションがバージョン 3.3.0 ビルド 31 前に CRWS のあらゆるバージョンと提供されたデフォルト IOSコンフィギュレーションに基づいていた次の Ciscoルータはこの脆弱性から影響を受けるかもしれません:

- Cisco 806
- Cisco 826
- Cisco 827
- Cisco 827H
- Cisco 827-4V
- Cisco 828
- Cisco 831
- Cisco 836
- Cisco 837
- Cisco SOHO 71
- Cisco SOHO 76
- Cisco SOHO77
- Cisco SOHO 77h
- Cisco SOHO78
- Cisco SOHO 91
- Cisco SOHO 96
- Cisco SOHO 97

脆弱性を含んでいないことが確認された製品

IOSコンフィギュレーションが CRWS アプリケーションと提供されたデフォルト IOSコンフィギュレーションに基づいていない以前にリストされた Ciscoルータのうちのどれかが脆弱ではないです。

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 1.1	2006 August 10 1400 UTC（GMT）	固定 CRWS を含む新しいデバイスに追加された情報はリリースします。
リビジョン 1.0	2006 年 July 12 1600 UTC（GM	初回公開リリース

	T)	

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、単独の転載や意訳を施した場合、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。