

Cisco Secure ACS for Windows における Web インターフェイスの脆弱性

severity	アドバイザリーID : cisco-sa-20020403-acs-win-web	CVE-2002-0160
	初公開日 : 2002-04-03 16:00	0160
	バージョン 1.1 : Final	CVE-2002-0159
	回避策 : Yes	0159
	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

Windows のための Cisco Secure Access Control Server (ACS) は 2 脆弱性が含まれています。1 脆弱性は ACS サーバの任意のコードの実行の原因となり第 2 は情報の無許可の開示の原因となる場合があります。パッチは両方の脆弱性に利用できます。

Cisco Secure ACS for UNIX は脆弱ではありません。その他のCisco製品は脆弱ではありません。

脆弱性のための直接回避策がありませんが、それらを大いに軽減することは可能性のあるです。詳細については[回避策](#) セクションを参照して下さい。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020403-acs-win-web> で利用できます。

該当製品

修正済みソフトウェア

影響を受けた製品は Cisco Secure Access Control Server for Windows です; 2.6.x および ACS 3.0.1 以前のすべてのリリース (ビルドは 40) 影響を受けています。

脆弱性を含んでいないことが確認された製品

Cisco Secure ACS for UNIX は影響を受けていません。

他のシスコ製品においてこのアドバイザリー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	2002-April-05	該当製品に行われる更新およびソフトウェア バージョン および 修正。
リビジョン 1.0	2002-April-03	初版リリース

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。