Cisco Secure Access Control System パスワード修正脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20110330-CVE-2011-0951 **初公開日 :** 2011-03-30 16:24 **バージョン 1.0 :** Final **CVSSスコア :** 5.0 **回避策 :** Yes **Cisco バグ ID :**	CVE-2011-0951

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 Secure Access Control System （ ACS ）は非認証を可能にする可能性があるユーザパスワードを修正するために脆弱性がリモート攻撃者含まれています。

脆弱性は Cisco Secure ACS アプリケーションのウェブベースの管理インターフェイスのユーザパスワード変更機能の不適当なセキュリティ制限が原因です。 非認証はシステムへ悪意のある要求を送信 することによって、リモート攻撃者この脆弱性を不正利用する可能性があります。 成功すれば、攻撃者はユーザアカウント パスワードを修正する可能性があります。

Cisco は Security Advisory のこの脆弱性を確認し、更新済ソフトウェアをリリースしました。

この脆弱性を不正利用するために、攻撃者はターゲットのシステムに悪意のある要求を送信できる必要があります。 攻撃者は内部ネットワークにアクセスがエクスプロイトを達成するように要求するかもしれません。

Cisco は CVSS スコアを通してその機能エクスプロイト コード存在を示します; ただし、コードは共用利用可能であると知られていません。

該当製品

修正済みソフトウェア

次の Cisco Secure ACS バージョンはこの脆弱性から影響を受けます。 製品のハードウェアアプライアンスおよびソフトウェアのみのバージョンは両方脆弱です。

- インストールされるインストールされるこれらのパッチのパッチ 3、4、か 5（またはあらゆる組み合せの）およびパッチ 6 またはそれ以降のない Cisco Secure ACS バージョン 5.1
- パッチがインストールされていない Cisco Secure ACS バージョン 5.2
- インストールされるインストールされるパッチ 1 か 2（または両方のパッチが付いている）およびパッチ 3 またはそれ以降のない Cisco Secure ACS バージョン 5.2

脆弱性を含んでいないことが確認された製品

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

バージョン	説明	Section	ステータス	日付
1.0	初版リリース	該当なし	Final	2011-Mar-30

利用規約