Cisco Secure Access Control Server EAP-TLS 認証の脆弱性

severity	**アドバイザリーID :** cisco-sa-20041102-acs-eap-tls	CVE-2004-1099
	初公開日 : 2004-11-02 15:00	
	バージョン 1.0 : 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

拡張可能認証プロトコル転送する 層 セキュリティ（EAP-TLS）をネットワークにユーザを認証するのに使用するように設定される Cisco Secure Access Control Server （ACS）はユーザネームが有効である限り暗号に正しい認証を使用するあらゆるユーザにアクセスを許可します。 認証が適切な形式にある含まれています有効なフィールドを*訂正して下さいことを暗号*に意味し。 認証はまだ信頼できない認証局（CA）から期限切れです、または来るおよび暗号に正しい場合もあります。

Cisco Secure ACS for Windows および Cisco Secure ACS ソリューション エンジンのバージョン 3.3.1 だけこの脆弱性から影響を受けます。 Cisco はこの問題を提起するためにフリーソフトを使用できるようにしました。

この脆弱性は効果をもたらしません、すなわち、ユーザ認証は EAP-TLS が唯一の比較メソッドでユーザ許可証のバイナリ比較で Cisco Secure ACS で設定されれば、そして Lightweight Directory Access Protocol（LDAP）/アクティブ ディレクトリ（LDAP/AD）の User エントリが有効な証明書だけ含まれていれば、影響を与えられません。

この脆弱性の不正利用は報告されませんでした。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20041102-acs-eap-tls で利用できます。

該当製品

修正済みソフトウェア

Cisco Secure ACS for Windows および Cisco Secure ACS ソリューション エンジンのバージョン 3.3.1 だけこの文書に説明がある脆弱性から影響を受けます。

Cisco Secure ACS Software バージョンを判別するために Cisco Secure ACS にログイン することができます。 最初の画面 正常なログインが次の形式でバージョン番号を示した後示される: `CiscoSecure ACS 3.3(1) 16`。

ACS バージョンはまた `003.003(001.16)` として「`16`" ACS 管理 グラフィカル ユーザ インターフェイス（GUI）で参照されるビルド 番号であるところに表示するかもしれません。

脆弱性を含んでいないことが確認された製品

Cisco Secure ACS for Windows および Cisco Secure ACS ソリューション エンジンの Cisco Secure ACS for UNIX およびバージョンは前の、およびそれ以降より、この脆弱性から 3.3.1 **影響を受けません。** バージョン 3.3.1 は 3.3.x シリーズの最初のバージョンであり、バージョン 3.3.2 はこの脆弱性から影響を受けない最初のものです。 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 1.0	2004-November-02	初回公開リリース

利用規約