UNIX VPN Client のバッファオーバーフロー

severity	**アドバイザリーID :** cisco-sa-20020619-unix-vpn-buffer-overflow	CVE-2002-1447
	初公開日 : 2002-06-19 14:00	
	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

Linux、Solaris および Mac OS X プラットフォームのための Cisco VPN Client のバッファオーバーフローがクライアント システムの管理権限を得るのにローカルで不正利用することができます。 脆弱性は vpnclient バイナリ実行可能なファイルの「setuid」権限を取除くことによって軽減することができます。 Windows プラットフォームのための Cisco VPN Client は影響を受けていません。

脆弱性はバージョン 3.5.2 で修復されました。 Cisco は修正済みソフトウェアを影響を受けた顧客に使用できるように自由にしています。 この問題は **CSCdx39290** として文書化されています。 Cisco はこの脆弱性の公の議論かアクティブな利用に気づいていません。

この Security Advisory の公式 最新のコピーは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020619-unix-vpn-buffer-overflow で利用できます。

該当製品

修正済みソフトウェア

この脆弱性は Linux、Solaris および Mac OS X プラットフォームのための Cisco VPN Client のバージョン 3.5.1 および それ 以前に影響を与えます。

脆弱性を含んでいないことが確認された製品

この脆弱性はあらゆる Windows プラットフォームのための Cisco VPN Client に影響を与えません。

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	2002-June-19	初回公開リリース

利用規約