Cisco VPN 5000 シリーズ コンセントレータ RADIUS PAP 認証脆弱性

severity	**アドバイザリーID :** cisco-sa-20020807-vpn5k-radius-pap **初公開日 :** 2002-08-07 15:00 **バージョン 1.0 :** Final **回避策 :** Yes **Cisco バグ ID :**	CVE-2002-0848

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

Remote Authentication Dial In User Service （RADIUS）サーバをクライアント接続を認証するのに使用するように VPN 5000 シリーズ コンセントレータが設定されるおよび選択される身元証明要求タイプが Password Authentication Protocol （PAP）または身元証明要求（PAP のハイブリッド）である時、検証が最初に暗号化してもらわない User Password フィールドをおよび失敗する従ってパスワードはクリアテキストとして送信されます場合の RADIUSサーバに送信 される検証リトライ要求。 Challenge Handshake Authentication Protocol （CHAP）を認証するのに使用するように設定される VPN 5000 シリーズ コンセントレータはこの脆弱性から影響を受けません。

この脆弱性は Cisco バグ ID CSCdx82483 として文書化されています。 利用可能 な 回避策がこの脆弱性の影響を軽減するためにあります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020807-vpn5k-radius-pap で掲示されます。

該当製品

修正済みソフトウェア

ソフトウェア リリース 6.0.21.0002 （およびそれ以前）および 5.2.23.0003 を実行するすべての Cisco VPN 5000 シリーズ コンセントレータ ハードウェアはこの脆弱性から（およびそれ以前）影響を受けます。 このシリーズはモデル 5001、5002、および 5008 が含まれています。

より古い IntraPort シリーズ コンセントレータ ハードウェアはまたこの脆弱性から影響を受けます。 このシリーズはモデル IntraPort 2、IntraPort 2+、IntraPort Enterprise-2 および Enterprise-8、IntraPort Carrier-2、および Carrier-8 が含まれています。

VPN 3000 シリーズ コンセントレータ ハードウェアは影響を受けていません。

ソフトウェアリビジョンを確認するために、**show version コマンド**を使用してコマンド ライン インターフェースによって修正をチェックして下さい。

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

リビジョン 1.0	2000-August-07	初回公開リリース

利用規約