VPN 3000 コンセントレータ IP オプション脆弱性

severity

アドバイザリーID : cisco-sa-20010412-vpn3kipoptions

初公開日 : 2001-04-12 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

無効なIP オプション設定との巧妙に細工された IPパケットが、同じネットワークセグメント（中間ルータ無し）の VPN 3000 シリーズ コンセントレータに送信されれば、により VPN 3000 シリーズ コンセントレータは 100% CPU稼働率とハングします場合があります。 コンセントレータはそれからリセットされなければなりません。 リブートの後で、機器は巧妙に細工された IPパケットが再度受け取られるまで普通機能します。 問題がサービス拒絶（DoS）攻撃を生成 するのに利用することができます。

脆弱性は Cisco バグ ID CSCds92460 に説明があります。

この表記は http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010412-vpn3kipoptions で掲示されます

該当製品

修正済みソフトウェア

Revision 2.5.2(f) より前ソフトウェア リリースを実行する Cisco VPN 3000 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す。 このシリーズはモデル 3005、3015、3030、3060、および 3080 が含まれています。

Cisco VPN 3000 シリーズ コンセントレータが影響を受けたソフトウェアを実行したかどうか確認するために、Webインターフェイスか Console メニュー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

Revision 2.5.2(f) またはそれ以降を実行するどの VPN 3000 シリーズ コンセントレータでもこの脆弱性によって変化しないです。

この脆弱性は VPN 5000 シリーズ コンセントレータに影響を与えません。 その他のCisco製品はこの脆弱性から影響を受けるために知られていません。

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	2001-April-12	初回公開リリース

利用規約