Cisco VPN 3000 Concentrator の 脆弱性

severity

アドバイザリーID : cisco-sa-20030507-vpn3k

初公開日 : 2003-05-07 16:00

バージョン 1.2 : Final

回避策 : Yes

Cisco バグ ID :

CVE-2003-0260

CVE-2003-0258

CVE-2003-0259

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

このアドバイザリは Cisco VPN 3000 シリーズ コンセントレータおよび Cisco VPN 3002 Hardware Client のための脆弱性を文書化します。 これらの脆弱性は Cisco バグ ID CSCea77143（IPSec over TCP）、CSCdz15393（SSH）、および CSCdt84906（ICMP）として文書化されています。 これらの脆弱性に対しては、影響を緩和するための回避策があります。 、バージョン 4.0.1 および 3.6.7F は Cisco VPN 3000 シリーズ コンセントレータおよび Cisco VPN 3002 Hardware Client のためのコードのバージョンにアップグレードしてこれらの文書化された脆弱性すべてから、保護します。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030507-vpn3k で掲示されます。

該当製品

修正済みソフトウェア

Cisco VPN 3000 シリーズ コンセントレータはこれら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、3080 および Cisco VPN 3002 Hardware Client が含まれています。

DDTS - 説明	該当するリリース
CSCea77143 - IPSec over TCP 脆弱性を有効に する こと	• 4.0.REL • 3.6.REL による 3.6.7E

	• 3.5.x • 3.1.x、3.0.x および 2.x.x は影響を受けていません。
CSCdz15393 -不正 な SSH 初期化 パケットの脆弱性	• 3.6.6 による 3.6.REL • 3.5.x • 3.1.x • 3.0.x • 2.x.x
CSCdt84906 -不正 な ICMP トラフィック脆弱性	• 3.6.7 による 3.6.REL • 3.5.x • 3.1.x • 3.0.x • 2.x.x

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 メニューによってソフトウェアリビジョン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

これらの脆弱性は VPN Client ソフトウェア Cisco VPN 5000 シリーズ コンセントレータ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	2003-May-7	初回公開リリース
リビジョン 1.1	2003-May-7	該当製品 表を訂正しました。
リビジョン 1.2	2003-May-8	修正済みソフトウェア取得のセクションのリンクを訂正しました。

利用規約

情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。