

VPN3000 コンセントレータ の TELNET 脆弱性

severity アドバイザリーID : cisco-sa-20010328-vpn3k-telnet
初公開日 : 2001-03-28 16:00
バージョン 1.1 : 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

SSL または規則的なtelnet ポートへ膨大なデータを送信 するにより Cisco VPN 3000 シリーズ コンセントレータはリブートします場合があります。 リブートの後で、機器は膨大なデータが再度送信 されるまで普通機能します。

脆弱性を取除くために、Cisco はすべての影響を受けたプラットフォームのための Revision 2.5.2(f) に無償ソフトウェアアップグレードを提供しています。問題はコンパニオン DDTS CSCds90807 および CSCds64223 に説明があります。

この表記は <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010328-vpn3k-telnet> で掲示されます

該当製品

修正済みソフトウェア

バージョン 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。どのモデル実行バージョン 2.5.2(F) または それ以降でもこの脆弱性によって変化しないです。

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コンソールログインによってバー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 1.1	2001- March-30	修正済みソフトウェアの修正で変更して下さい
リビジョン 1.0	2001- March-28	初回公開リリース

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な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。