VPN3000コンセントレータのTELNETの脆弱性

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 : No Workarounds available
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または通常のTelnetポートに大量のデータを送信すると、Cisco VPN 3000シリーズコンセントレータがリブートする可能性があります。リブート後、大量のデータが再送信されるまで、機器は正常に機能します。

この脆弱性を排除するため、シスコでは該当するすべてのプラットフォームに対して、リビジョン2.5.2(F)への無償ソフトウェアアップグレードを提供しています。この不具合はコンパニオンDDTSのCSCds90807およびCSCds64223で説明されています。

この Notice は https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010328-vpn3k-telnet で公開されます。

該当製品

このセクションには、該当製品に関する詳細が掲載されています。

脆弱性のある製品

バージョン2.5.2(F)以前のソフトウェアリリースを実行しているCisco VPN 3000シリーズコンセントレータは、この脆弱性の影響を受けます。このシリーズには、モデル3005、3015、3030、3060、および3080が含まれます。バージョン2.5.2(F)以降を実行しているモデルは、この脆弱性の影響を受けません。

Cisco VPN 3000シリーズコンセントレータで該当のソフトウェアが実行されているかどうかを確認するには、Webインターフェイスまたはコンソールログインを使用してバージョンをチェックします。

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、VPN 5000シリーズコンセントレータには影響しません。他のシスコ製品はこの脆弱性の影響を受けません。

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。

詳細

この脆弱性は、SSLまたは通常のTelnetセッションが失敗を繰り返した後に接続解除されず、システムがSSLまたは通常のTelnetポートで受信したデータの解釈を試行し続けることによって発生します。そのため、制御不能なレートで受信されるデータによってtelnetキューがフラッディングされ、システム上のメモリ不足が引き起こされ、リブートが発生する可能性があります。この問題は、SSLまたは通常のTelnetセッションが3回失敗した後に確実に終了することで修正されています。この脆弱性は、2つのコンパニオンDDTSのCSCds90807およびCSCds64223で文書化されています。

回避策

この脆弱性は、アップグレードするまで機器へのTelnetアクセスをすべて無効にすることで回避できます。

特定のインターフェイスでtelnetを許可しない場合は、2つの方法があります。1つは、telnetを許可しないルールが設定されたフィルタを使用する方法です。もう1つは、telnetアクセスを明示的に拒否するルールを作成し、それを既存のフィルタに適用する方法です。

詳細については、
http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/vpn3kco/vcoug/usr_3_0/polmgt.htmを参照してください。

SSLと通常のTelnetを無効にした後は、コンソールポートまたはブラウザアクセスを介して機器を管理できます。

修正済みソフトウェア

この脆弱性は、リビジョン2.5.2(F)コードで修正されています。修正は今後のすべてのリリースに適用されます。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。これは、SSL Telnetツールを使用した副作用としてこの脆弱性を発見したお客様からシスコに報告されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010328-vpn3k-telnet

改訂履歴

リビジョン 1.1	2001年3月30日	修正済みソフトウェアのリビジョン変更
リビジョン 1.0	2001年3月28日	初回公開リリース

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。