Cisco Catalyst メモリリークの脆弱性

severity

アドバイザリーID : cisco-sa-20001206-catalyst-memleak

初公開日 : 2000-12-06 16:00

バージョン 1.3 : 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

スイッチへの一連の壊れる telnet認証試みは Catalyst スイッチの原因になる場合がありますトラフィックを通過させるか、またはシステムがリブートされるか、または電源の再投入が実行されたまで管理接続を許可しないために。 telnet認証のすべての型は Kerberos 対応 の Telnet および AAA認証を含んで影響を受けています。

この脆弱性は Cisco バグ ID **CSCds66191 を**割り当てられました。

完全なアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20001206-catalyst-memleak で表示することができます。

該当製品

修正済みソフトウェア

脆弱性を含む製品は次のとおりです。

- 5.5(4) および 5.5(4a) までバージョン 4.5(2)を実行する Catalyst 4000 および 5000 イメージ。
- 5.5(4) および 5.5(4a) 以前でバージョン 5.3(1)CSX を、実行する Catalyst 6000 イメージ。
- バージョン 6.1(1)b および 6.1(2)は脆弱性のためのテストで影響を受けませんでした; ただし、コード修正は予防処置としてそれらのリリースに含まれていました。
- Catalyst 5000 シリーズ イメージは Catalyst 2901 で、2902、2926T、2926F、2926GL、2926GS 固定設定 シャーシ、および 5000、5002、5500、5505、および 5509 のモジュラーシャーシ スイッチ インストールされています。
- Catalyst 4000 シリーズは Catalyst 2948G で、2980G、4003、4006、および 4912G スイ

ッチ インストールされています。
- Catalyst 6000 シリーズは Catalyst 6009、6006、6509、6509-NEB および 6506 のモジュラーシャーシ スイッチでインストールされています。
- Catalyst 2900XL プラットフォームはこの脆弱性から影響を受けません。

脆弱性を含んでいないことが確認された製品

Cisco Catalystソフトウェアの他のリリースはこの脆弱性から影響を受けしません。 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 1.3	2000-December-20	更新済該当製品リスト。
リビジョン 1.2	2000-December-11	詳細 セクションのスイッチのメモリを監視するのに使用することができる" show mbuf total " コマンドの追加された詳細。
リビジョン 1.1	2000-December-07	該当製品およびソフトウェア バージョン および 修正セクションの Catalystソフトウェア バージョン 6.1(1)b についての追加された情報および 6.1(2)。
リビジョン 1.0	2000-December-06	初回公開リリース

利用規約