Cisco CatOS Embedded HTTP Server でバッファがオーバーフローする脆弱性

severity

アドバイザリーID : cisco-sa-20021016-catos-http-overflow

初公開日 : 2002-10-16 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

Cisco CatOS ソフトウェアの特定のバージョンが稼働している Cisco Catalyst スイッチは組み込み HTTPサーバのバッファオーバーフローに脆弱です。 イメージ名で「cv」が含まれている 7.3 以前の 5.4 からの CatOS バージョンだけ影響を受けています。 HTTPサーバが有効に なれば スイッチの失敗し、リロードするために原因になるバッファオーバーフローはリモートで不正利用することができます。 脆弱性は繰り返し不正利用され、サービス拒否という結果に終る場合があります。

回避策は利用できますこと制限脆弱性を不正利用する機能。 このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20021016-catos-http-overflow で公開されます。

該当製品

修正済みソフトウェア

この脆弱性は CiscoView Network Management Software をサポートするために組み込み HTTPサーバが含まれている 7.3 によって Cisco CatOS ソフトウェア バージョン 5.4 が稼働している Cisco Catalyst スイッチにだけあります。 影響を受けたソフトウェア イメージはここに見られるようにイメージ名で「cv」が含まれています: cat6000-supcv.5-5-16.bin.

脆弱性を含んでいないことが確認された製品

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

リビジョン番号 1.1	2002-October-17	「ソフトウェア バージョン および 修正」セクションを「まだ固定として」。リストされていたソフトウェア バージョン 7.3 を取除くためにアップデートしました
リビジョン番号 1.0	2002-October-16	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、単独の転載や意訳を施した場合、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。