

CBOS - サービス拒否攻撃への弾性の改善

severity アドバイザリーID : cisco-sa-20020523-cbos-dos

初公開日 : 2002-05-23 16:00

バージョン 1.2 : 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

3 新しい脆弱性は Cisco Broadband Operating System (CBOS) で、ルータの Cisco 600 ファミリー用のオペレーティングシステム識別されます。各脆弱性により Customer Premises Equipment (CPE) のフリーズによってサービス拒否 (DoS) を引き起こす場合があります。3 脆弱性はすべてリモートで不正利用することができます。

その他のCisco製品は脆弱ではありません。

回避策は 3 脆弱性の 2 に提供されます。提供される回避策がいずれの場合も適当ではないかもしれないことに注目して下さい。更に詳しい情報については[回避策](#) セクションを参照して下さい。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020523-cbos-dos> で利用できます。

該当製品

修正済みソフトウェア

2.4.4 リリース以前で CBOSソフトウェアを実行している 600 ファミリーからのすべての Cisco DSL CPE デバイスは脆弱です。脆弱なハードウェアモデルの完全なリストは次のとおりです: 626、627、633、673、675、675e、676、677、677i および 678。

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ー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 1.2	2002-June-17	更新済ソフトウェア バージョン および 修正 セクション
リビジョン 1.1	2002-May-31	更新済 Affected Products セクション
リビジョン 1.0	2002-May-23	初版リリース

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。