

TFTP ロング ファイル名の脆弱性

severity アドバイザリーID : cisco-sa-[CVE-20020730-ioc-tftp-lfn](#)
初公開日 : 2002-07-30 18:00 [2002-0813](#)
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

トリビアル ファイル転送プロトコル (TFTP) はプロトコルですネットワーク 接続装置間のファイルの容易な転送のために可能にする。脆弱性は IOSデバイスおよび PXM-1 によって基づく MGX スイッチの TFTP 読み取り要求内のファイル名の処理で検出されました。

以下の製品はこの脆弱性から影響を受けるように指定されます:

- MGX 8230 は、8250 および PXM-1 はバージョン 1.2.10 または それ以前が稼働している MGX 8850 スイッチを基づかせていました
- バージョン 11.1 を、11.2 実行する、Cisco IOSデバイス 11.3

明示的に別の方法で示されて、すべてのその他のCisco製品は影響を受けていません。

MGX スイッチに回避策がありません。

IOSデバイス、存在 する [回避策](#) 下記の例で詳述される簡単な回避策。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020730-ioc-tftp-lfn> で利用できます。

該当製品

修正済みソフトウェア

以下の製品は影響を受けています:

- MGX 8230 は、8250 および PXM-1 はバージョン 1.2.10 または それ以前が稼働している MGX 8850 スイッチを基づかせていました

- バージョン 11.1 を、11.2 実行する、Cisco IOSデバイス 11.3

脆弱性を含んでいないことが確認された製品

以下の製品は影響を受けていません:

- MGX 8830 スイッチ
- 基づく PXM-1 ではない MGX 8850 スイッチ
- ルートプロセッサのような 68040 基づいたアーキテクチャで動作した場合 Cisco IOS ソフトウェア バージョン 11.1、11.2、11.3。

この特定のアーキテクチャだけ上の一般に影響を受けたバージョンのリロードに脆弱ではないです。Route Switch Processors のようなその他のデバイスは影響を受けています。ルートプロセッサのどの型があるか確認するために、コマンド **show version** をルータのプロンプトで発行し、に類似したストリングを探して下さい:

```
cisco RP1 (68040) processor (revision A0) with 16384K bytes of memory.
```

- IOSソフトウェアバージョン 12.0 を実行する IOSデバイス以上に

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	2003-August-20	MGX スイッチ用の訂正された ID 番号
リビジョン 1.2	2003-August-14	MGX スイッチについての情報を追加しました
リビジョン 1.1	2002-August-20	公示の信じられた脆弱性レポーター
リビジョン 1.0	2002-July-30	初版リリース

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。