脆弱性スキャン後 の IOS リロード

severity

アドバイザリーID : cisco-sa-20010524-ios-tcp-scanner-reload

初公開日 : 2001-05-24 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

セキュリティ スキャン ソフトウェアによりリロードが発生します Cisco IOSÂ® ソフトウェアで記憶誤 りを引き起こす場合があります。 この脆弱性はそれらのバージョンに基づいて Cisco IOS ソフトウェア バージョン 12.1(2)T および 12.1(3)T、および限定配備リリースだけ該当します。

該当する Cisco IOS ソフトウェア リリースを使用している顧客はこの問題に脆弱ではない以降のバージョンにできるだけ早くアップグレードするように勧められます。 脆弱性が存在する製品およびリリースは下記に詳しくリストされています。

セキュリティスキャナは更にある決まったポートと対応づけられたそれらのサービスを用いる既知の脆弱性を調査するために開港を探すさまざまなポートに TCP 接続の試みを試みます。 ただし、テストの副次的影響はこの Security Advisory に説明がある問題を露出しコンフィギュレーション ファイルを検討するか、または書く要求を受け取るとすぐルータは予想に反してリロードします。

この問題は Cisco バグ ID CSCds07326 として文書化されています。

完全な表記は http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010524-ios-tcp-scanner-reload で利用できます。

該当製品

修正済みソフトウェア

この表記のすべてのシスコ製品をリストすることは不可能です; リストは下記の広く使われたのかほとんどの問い合わせのあるプロダクトだけ含まれています。

デバイスは Cisco IOSソフトウェアを実行しているかどうか不確実、デバイスにログイン し、コマンド **show version を**発行して下さい。 Cisco IOSソフトウェアは「IOS」か「インターネットワーク オペレーティング システム ソフトウェア」としてそれ自身を単に識別します。 他の Ciscoデバイスに **show version コマンドが**ありませんし、別の出力を与えません。

Cisco IOSソフトウェアを実行する Ciscoデバイスは次が含まれています:

- AGS/MGS/CGS/AGS+ の Ciscoルータ、IGS、RSM、8xx、ubr9xx、1xxx、25xx、26xx、30xx、36xx、38xx、40xx、45xx、47xx、AS52xx、
- AS53xx、AS58xx、64xx、70xx、72xx（を含む ubr72xx）、75xx および 12xxx シリーズ。
- LS1010 ATM スイッチのほとんどの最近のバージョン。
- Catalyst 2900XL LAN スイッチのバージョン。
- Cisco DistributedDirector。

影響を受けたソフトウェア バージョンは比較的新しく、必ずしも上記リストに記載されている各デバイスで利用できません。

脆弱性を含んでいないことが確認された製品

Cisco IOSソフトウェアを実行しない場合、この脆弱性から影響を受けません。 Cisco IOSソフトウェアを実行しない Ciscoデバイスはこの脆弱性から、含まれています次が影響を受けないし:

- 7xx ダイヤルアップルータ（750、760、および 770 シリーズ）は影響を受けていません。
- Catalyst 19xx、28xx、29xx、3xxx および 5xxx LANスイッチは Catalyst 2900XL のバージョンを除いて影響を受けていません。 ただし、Catalyst 5000 および 5500 のための RSM モジュールのようなスイッチ バックプレーンの Cisco IOSソフトウェアを、実行するオプションのルータ モジュールは影響を受けています。
- IGX および BPX 行の WANスイッチングプロダクトは影響を受けていません。
- MGX は（以前 AXISシェルフとして知られている）影響を受けていません。
- ホストベース ソフトウェアは影響を受けていません。
- Cisco PIX Firewall は影響を受けていません。
- Cisco LocalDirector は影響を受けていません。
- Cisco Cache Engine は影響を受けていません。
- Cisco CSS 11000 シリーズ スイッチは影響を受けていません

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 1.1	2001-May-24	回避策 セクションへの行われた変更を
リビジョン 1.0	2001-May-24	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。