

# Cisco IOSソフトウェア TELNET オプション 処理の脆弱性

severity アドバイザリーID : cisco-sa-20000420-ios-telnet

初公開日 : 2000-04-20 13:00

バージョン 1.0 : 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

ルータがセキュリティスキャンソフトウェアプログラムによってセキュリティーの脆弱性のためにテストされる場合複数の Cisco IOS ソフトウェアバージョンの問題により Cisco ルータは予想に反してリロードします。問題が一貫したサービス拒絶 (DoS) 攻撃を生成するのに繰り返し利用することができます。

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ある特定の UNIX ベースのシステムに影響を及ぼす 2 特定の脆弱性の存在のためにテストしています。脆弱性は Cisco IOS ソフトウェアに無関係であり、Cisco IOS ソフトウェアは直接それらから危険な状態にありません。ただし、テストの効果はこの Security Advisory に説明がある問題を露出し後続のトラフィックを受信す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 CSCdm70743 として文書化されています。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20000420-ios-telnet> で掲示されます。

## 該当製品

### 修正済みソフトウェア

次の Cisco IOSソフトウェアのメジャーリリースはこの問題に脆弱です:

- 11.3AA
- 12.0 リリース: 12.0(2) 以前の 12.0(6)
- 12.0(7)、但し例外としては 12.0(7)S、12.0(7)T および 12.0(7)XE は脆弱ではないです

この脆弱性は影響を受けたソフトウェアを実行する場合以下の Ciscoハードウェアプロダクトに影響を及ぼします:

- AS5200、AS5300 および AS5800 シリーズ アクセス サーバ
- 7200 および 7500 シリーズ ルータ
- ubr7200 シリーズ ケーブルルータ
- 7100 シリーズ ルータ
- 3660 シリーズ ルータ
- SC3640 システムコントローラ ( 後で説明を参照して下さい )
- AS5800 シリーズ 音声ゲートウェイ 製品
- AccessPath LS-3、TS-3 および VS-3 アクセスソリューション 製品

SC3640 システムコントローラは複数のアクセス サーバのローカル管理を提供するためにカスタマイズされる Cisco 3640 ルータです。Cisco SC3640 バイナリイメージはそれがデバイスに telnet に攻撃者のために可能性のあるである場合問題が含まれ、こうして脆弱です。ただし、オリジナル Cisco 3640 ルータは問題が含まれないし、この表記に説明がある DoS攻撃に脆弱ではないです。

## 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 バージョン 11.3、11.3T、11.2 または下部の、および 12.0(8) または 12.1 を実行している Ciscoカスタマーはまたはより高い影響を受けていません。Cisco IOSソフトウェアの特定のリリースに関する詳細および推奨される アップグレード パスはセクション「[ソフトウェア バージョン および 修正](#)」で下記に与えられます。

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

1.0	2000-April-20	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。