

Cisco ガードおよびトラフィック異常探知器のデフォルト 管理パスワード

severity アドバイザリーID : cisco-sa-20041215-guard

初公開日 : 2004-12-15 19:00

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

Cisco ガードおよび Cisco トラフィック異常探知器ソフトウェアは管理者アカウントのためのデフォルトパスワードが含まれています。このパスワードは Cisco ガードおよびトラフィック異常探知器分散型サービス拒否 (DDoS) 軽減アプライアンスによって使用されるソフトウェアのインストールの間に、あらゆるユーザの介入なしで、設定され製品のすべてのインストールに同じです。

Cisco ガードおよびトラフィック異常探知器のソフトウェアバージョン 3.0 およびそれ以前はこの脆弱性から影響を受けます。ソフトウェアのバージョン 3.1 またはそれ以上を実行している顧客は影響を受けていません。利用可能な回避策がありまデバイスの再度ブートするを必要としない 1 つが含まれています。Cisco はこの問題を提起するためにフリーソフトを使用できるようにしました。

脆弱性は Cisco バグ ID 次のように文書化されています: [CSCeg12167](#) ([登録ユーザのみ](#)) および [CSCeg12188](#) ([登録ユーザのみ](#))。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20041215-guard> で利用できます。

該当製品

修正済みソフトウェア

バージョン 3.1 前の Cisco ガードおよび Cisco トラフィック異常探知器のためのソフトウェアのすべてのバージョンはこの脆弱性から影響を受けます。

Cisco ガードおよび Cisco トラフィック異常探知器 DDoS 軽減アプライアンスが実行しているソフトウェアバージョンを判別する 3 つの方法があります:

- 仮想端末装置またはローカル シリアルコンソール接続
- 遠隔セキュア シェル (SSH) 結合
- リモート セキュア Web セッション

続くものが各メソッドの例です; 特定の環境およびネットワーク セットアップに適用するメソッドを選択する必要があります。

1. ソフトウェアバージョン番号をアプライアンスに接続するのにローカル シリアルコンソールを通して判別するためにシリアルケーブルおよび終端エミュレーションプログラムを使用して下さい。接続されたらターミナルの入力 キーを押せばガードおよびトラフィック異常探知器は、ログオンしないで、デバイスで動作するソフトウェアのバージョンを示します:

```
Cisco Guard Version 3.1(0.12)
```

GUARD login: この例で Cisco ガードはソフトウェア バージョン 3.1 を実行しています。仮想端末装置に関してはプロシージャは同じです但し例外としてはシリアルケーブルか終端エミュレーションプログラムは必要ではありません (標準キーボードおよびモニタはアプライアンスに直接接続されます。)

2. ソフトウェアバージョン番号を Cisco ガードまたは Cisco トラフィック異常探知器にログインし、**show version** Command Line Interface (CLI) コマンドを発行するのに SSH セッションによって得るために SSH クライアントを使用して下さい。次の例は Cisco トラフィック異常探知器との相互対話を示したものです:

```
prompt$ ssh admin@detector.example.com
admin@detector.example.com's password:
Last login: Wed Nov 24 22:45:53 on ttyS0
admin@DETECTOR#show version
Copyright (c) 2000-2004 Cisco Systems, Inc. All rights reserved.
```

```
Software License Agreement
```

```
[...]
```

```
Cisco Anomaly Detector
Release: 3.1(0.12)
Date: 2004/10/27 19:58:14
```

```
DETECTOR uptime is 3 weeks, 3 days, 17 hours, 53 minutes
System Serial Number: XXXXXXXX
```

```
Contact Information:
Cisco Systems Inc.
riverhead-support@cisco.com
```

admin@DETECTOR# この例で Cisco トラフィック異常探知器はソフトウェア バージョン 3.1 を実行しています。

3. Cisco ガードおよび Cisco トラフィック異常探知器がセキュア Web インターフェイスを通して実行しているソフトウェアバージョンを得るために、Web ブラウザの `Detector>/` URL `https:// < IP`、ログイン開き、次にブラウザウィンドウの右上 セクションにある

リンクを約クリックして下さい。

脆弱性を含んでいないことが確認された製品

その他のCisco製品は現在これらの特定のデフォルト アカウント/パスワードを作成するために知られていません。

改訂履歴

リビジョン 1.0	2004-December-15	初回公開リリース
--------------	------------------	----------

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。