Cisco 異常検知と緩和対策 製品の TACACS+ 認証 バイパス

severity	**アドバイザリーID :** cisco-sa-20060215-guard **初公開日 :** 2006-02-15 16:00 **バージョン 1.1 :** Final **回避策 :** Yes **Cisco バグ ID :**	CVE-2006-0764

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 異常検知と緩和対策アプライアンスおよびサービスモジュールで使用されるソフトウェアのバージョン 5.0(1) および 5.0(3)の脆弱性は Terminal Access Controller Access Control System Plus （ TACACS+ ）が不完全に設定される場合許可されていないユーザが不正アクセスをデバイスに得るおよび/または特権を増やすことを可能にするかもしれません。

TACACS+ 認証はデフォルトでディセーブルにされ、正しく TACACS+ 認証のために設定されるデバイスはこの脆弱性から影響を受けません。

シスコでは、該当するお客様用に、この脆弱性に対応する無償ソフトウェアを提供しております。 この脆弱性に対しては、影響を緩和するための回避策があります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060215-guard で掲示されます。

該当製品

修正済みソフトウェア

この脆弱性は TACACS+ 認証を使用するためにデバイスが不完全に設定される場合 Cisco Catalyst 6500 スイッチ/Cisco 7600 ルータの Cisco ガードおよび Cisco トラフィック異常探知器アプライアンスおよび異常ガード モジュールおよびトラフィック異常探知器モジュールのためのソフトウェアのバージョン 5.0(1) および 5.0(3)に影響を与えます。 以下の事項に注意して下さい:該当するリリースとしてリストされていない原因である 5.0(2) は cisco.com に決してリリースされませんでした。

影響を受けたソフトウェア バージョンを実行し、TACACS+ 認証のために設定されるデバイスは認証、許可、アカウンティング（AAA）コマンドが TACACS+ 認証を規定 したものですが、設定が TACACS+ サーバを規定 する **tacacs-server host コマンドに**欠けていれば場合脆弱です。 すなわち、設定は次のコマンドがのどちらかまたは両方が含まれていれば:

```
aaa authentication login tacacs+ local
aaa authentication enable tacacs+ local
```

しかしない次のコマンド:

```
tacacs-server host <IP address of TACACS+ server>
```

デバイスは脆弱です。

注: 上記の **AAA認証**コマンドの「は TACACS+」認証方式の後で規定 される「ローカル」認証方式脆弱性に無関係です。 この認証方式は TACACS+ サーバが利用できなければフォールバックとして普通使用されるので示されています。 規定 された場合「TACACS+」認証方式が「ローカル」メソッドの前に（使用され、場合、の有無にかかわらず、「脆弱 な多分デバイスローカル」認証方式）設定は **tacacs-server host コマンドに**欠けています。

脆弱性を含んでいないことが確認された製品

Cisco ガードおよび Cisco トラフィック異常探知器はこの脆弱性からそれらが次のソフトウェア バージョンを実行する場合影響を受けません:

- 5.0 前の 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のバージョン。これにはあらゆる 3.x および 4.x リリースが含まれています。
- 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 バージョン 5.1 以上に。

バージョン 5.0(1) または 5.0(3)を実行する Cisco ガードまたは Cisco トラフィック異常探知器はすなわちデバイスが TACACS+ サーバに対してユーザを認証するために設定されないかまたは TACACS+ 設定が完了した影響を受けていません、tacacs-server host コマンドが設定にある場合。

注: TACACS+ 認証はデフォルトでディセーブルにされます。 明示的 な AAA設定が起こらなければ Cisco ガードおよび Cisco トラフィック異常探知器はローカルデータベース（「ローカル」認証方式。）に対して認証しますユーザを

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 1.0	2006-February-15	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。