Cisco IOS セキュア シェル（SSH）サーバの脆弱性

severity	**アドバイザリーID :** cisco-sa-20050406-ssh **初公開日 :** 2005-04-06 16:00 **バージョン 1.1 :** Final **回避策 :** Yes **Cisco バグ ID :** CSCed65778 , CSCed65285	CVE-2005-1020 CVE-2005-1021

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インターネットワーク オペレーティング システム（IOS）のある特定のリリース トレインは Â®、方法として Terminal Access Controller Access Control System Plus IOSデバイスの遠隔管理タスクを行うのに（TACACS+）と組み合わせて IOS セキュア シェル（SSH）サーバを使用するために設定されたとき可能性としては IOSデバイスがリソースおよびリロードを排出します場合がある 2 脆弱性が含まれているかもしれません。 これらの脆弱性の繰り返された利用はサービス拒否（DoS）状態という結果に終る場合があります。 Remote Authentication Dial In User Service（RADIUS）のような他の認証方式およびローカルユーザデータベースとの SSH の使用はまた影響を受けるかもしれません。

Cisco はすべての影響を受けた顧客向けのこれらの脆弱性に対処するためにフリーソフトを使用できるようにしました。 利用可能 な 回避策が脆弱性の効果を軽減するためにあります（回避策セクションを参照して下さい。）

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050406-ssh で掲示されます。

該当製品

修正済みソフトウェア

これらの問題はサポートする影響を与え、SSH サーバの機能性使用するために設定されます Cisco IOS の取りはずされたバージョンを実行する Ciscoデバイスに。

Cisco 製品で稼働しているソフトウェアを確認するには、デバイスにログインし、**show version** コマンドを発行してシステム バナーを表示します。 Cisco IOS ソフトウェアは「Internetwork Operating System Software」または単に「IOS」と表示されます。 イメージ名は「バージョンに」先行しているこの識別の直後かっこ（可能性のある次の行で）と IOSリリース名の間で表示する。 その他の Cisco デバイスには **show version** コマンドがないか、異なる出力が返されます。

次の例は C806-K9OSY6-M のインストール済みイメージ名前と IOS リリース 12.2(15)T14（リリース トレイン ラベル "12.2T"）を実行する Ciscoデバイスを識別したものです:

```
Router1> show version
Cisco Internetwork Operating System Software
IOS (tm) C806 Software (C806-K9OSY6-M), Version 12.2(15)T14, RELEASE SOFTWARE (fc4)
[...]
```

次 の 例は C2600-IK9OS3-M のイメージ名と IOS リリース 12.3(10)（リリース トレイン ラベル "12.3 メインライン」）を実行するデバイスを示します:

```
Router2> show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK9O3S3-M), Version 12.3(10), RELEASE SOFTWARE (fc3)
[...]
```

Cisco IOS リリース指名についてのその他の情報は http://www.cisco.com/warp/public/620/1.html で見つけることができます。

SSH プロトコルは次の IOSの一連のリリースで導入されました:

- IOS 12.0S（1）SSH バージョン
- IOS 12.1T（1）SSH バージョン
- IOS 12.2（1）SSH バージョン
- IOS 12.2T（1）SSH バージョン
- IOS 12.3T（2）SSH バージョン

（サポートされた場合）IOSデバイスが実行している IOSイメージが SSH プロトコルのサーバ側をサポートしたかどうか確認するために有効に なる、および使用される SSH プロトコル バージョンはグローバル な モードで（SSH がサポートされ、有効に なれば）、**show ip ssh コマンドを**かどうか使用します:

```
Router> show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

前の出力はサポートされている SSH プロトコル 主要なバージョンがあること SSH がこのデバイスで有効に なる IOS によって報告される SSH プロトコル バージョンの 1.有効値次のとおりであることを示したものです、:

- 1.5: SSH プロトコル バージョンだけ 1 有効に なります。
- 1.99: 有効に なる SSH プロトコル バージョン 1 互換性の SSH プロトコル バージョン

2。
- 2.0: SSH プロトコル バージョンだけ 2 有効に なります。

IOS の SSH バージョンに関する詳細については、次の URL をチェックして下さい: http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_ssh2.html。

注: SSH プロトコル バージョン 1 および 2 は相互運用できませんがプロトコルのどちらかのバージョンを使用しているクライアントからの接続を処理する方法を通常 SSH サーバは知っていますこれをするためにほとんどの場合サーバは明示的に設定されなければなりません。 プロトコル バージョン 1 の最新の修正は今切らされたインターネット技術特別調査委員会（IETF）草案で文書化されています "1.5" です。

show ip ssh コマンドは IOS リリース 12.1(1)T でもたらされました。 従ってこのコマンドが利用できないそれから使用中の IOSイメージ持たなければ SSH サーバ サポートをおよび場合このアドバイザリで論議される問題に脆弱ではないです。

詳細 セクションで見るので、この文書に説明がある SSH プロトコルのバージョンによって脆弱性の動作は IOSデバイスが使用していること決まることができます。 従って、この情報を得ることを上に示されているように **show ip ssh コマンドを**使用することは重要です。

SSH を次の出力サポートしない **show ip ssh コマンドが**イメージで実行される場合生成されます:

```
Router> show ip ssh
                ^
% Invalid input detected at '^' marker.

Router>
```

最終的には IOSデバイスで動作するリリースおよびイメージが SSH をサポートしても、SSH サーバは有効に ならないかもしれません。 次の例は有効に なる SSH サーバが（ない SSH をサポートするが、「SSH によってディセーブルにされる」メッセージに注意しなさい）デバイスの **show ip ssh コマンド**からの出力を示したものです:

```
Router> show ip ssh
SSH Disabled - version 1.5
%Please create RSA keys to enable SSH.
Authentication timeout: 120 secs; Authentication retries: 3
Router>
```

脆弱性を含んでいないことが確認された製品

IOS を実行しないか、IOS トレインを SSH サーバの機能性*なし*で実行するか、または SSH をサポートする*なし*で IOSバージョンを実行するデバイスはしかし有効に なる SSH サーバ影響を受けていません。

SSH 機能を実装する IOSの一連のリリースの詳細リストについては Affected Products セクションを参照して下さい。 特に、次の IOSの一連のリリースは SSH コードが含まれていません:

- 12.0 以前のすべての IOSバージョン。
- IOS 12.0（メインライン-「S」トレインは SSH をサポートし、影響を受けています。）
- IOS 12.1（メインライン-「T」トレインは SSH をサポートし、影響を受けています。）

12.3 メインラインは SSH サーバの機能性をサポートするがさらに、それはこの文書で論議される問題に*脆弱*ではないです。 他のすべてのリリースおよびトレインに関しては、ソフトウェア バージョン および 修正 セクションをチェックして下さい。

Cisco IOS XR は該当しません。

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	2005-May-03	- 12.3 が SSH をサポートするが、脆弱ではないですこと明白にして下さい。 -修正済みソフトウェアの更新済表。 - 12.1AZ は 12.1(22)EA1 に、ない 12.2(22)EA1 移行します。 -コントロール プレーン ポリシング例のアクセス制御リスト エントリを訂正して下さい。 - SSH バージョン 2 脆弱性（CSCed65778（登録ユーザのみ）が TACACS+ 以外認証方式を使用して）デバイスに影響を与えること明白にして下さい（RADIUS および口ーカルユーザデータベース、たとえば。）
リビジョン 1.0	2005-April-06	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。