AAAコマンド許可バイパス

Informational

アドバイザリーID : cisco-sa-20060125-aaatcl
初公開日 : 2006-01-25 16:00
バージョン 1.0 : Final
回避策 : No Workarounds available
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

これは、2006年1月25日16:00 UTC(GMT)に投稿された元のシスコベンダーの回答の更新です。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060125-aaatcl
最初に公開された時点から、当初は修正済みとして文書化されていたCisco IOSの一部のバージョンが、この脆弱性の影響を受けていることが判明しています。この新しい問題は、Cisco Bug ID CSCsd28570(登録ユーザ専用)で追跡されています。更新されたCisco IOSの「ソフトウェアバージョンと修正」の表はにあります。その他の関連情報は変更されません。

Cisco Internetwork Operating System(IOS)Authentication, Authorization, and Accounting（AAA；認証、認可、アカウンティング）のコマンド認可機能には脆弱性が存在します。この機能では、Tool Command Language(Tcl)execシェルから実行されたコマンドに対してコマンド認可チェックが実行されません。これにより、認証されたユーザが一部の設定でコマンド許可チェックをバイパスできるようになり、不正な権限昇格が発生する可能性があります。

AAAコマンド許可機能を実行していないデバイス、またはTcl機能をサポートしていないデバイスは、この脆弱性の影響を受けません。

COLT Telecomネットワークエンジニアリングセキュリティ担当シニアマネージャのNicolas Fischbach氏に、この問題をシスコに報告していただいたことに感謝いたします。

Cisco では、研究者と協力してセキュリティ脆弱性に関する調査を進め、製品レポートで発表することを常に歓迎しています。

追加情報

詳細

AAAコマンド許可機能を実行し、IOSがTcl機能をサポートしているデバイスは、この脆弱性の影響を受ける可能性があります。

IOS内でTcl機能を持つデバイスは、コマンド**tclsh**を受け入れ、コマンドラインインターフェイス(CLI)プロンプトをCLIプロンプトで(tcl)に戻します。例：

```
router#tclsh
router(tcl)#
```

デバイスがTcl機能をサポートしていない場合は、エラーメッセージまたは別の出力が表示されます。

CLIプロンプト内の(tcl)テキストは、ユーザがTclシェルモード内にあることを示します。

AAAコマンド許可用に設定されたシステムでは、**show running-configuration**の出力に次のようなコマンドラインが表示されます。

```
aaa authorization commands
```

例：

```
aaa authorization commands 15 default group tacacs+ none
```

この脆弱性の影響を受けるデバイスでは、Tclシェルモードからユーザ認証特権レベルで任意のIOS EXECコマンドを実行できます。この脆弱性は、次のバグIDに記載されています。

- CSCeh73049(登録ユーザ専用):tclshモードはAAAコマンド許可チェックをバイパスする
- CSCsd28570(登録ユーザ専用):AAA許可コマンドのtclshバイパス

この脆弱性を悪化させる別の問題が存在します（以下に記載）。前のユーザがTclシェルモードになり、Tclシェルモードを終了する前にセッションを終了した場合に限り、認証されたユーザは、**tclsh**コマンドを使用してTclシェルモードに手動で入力する中間ステップを実行することなく、自動的にTclシェルモードに入れられます(ルータプロンプト内に(tcl)の証拠はありません)。

特権ユーザがTclシェルを開始し、Tclシェルコマンド**tclquit**を発行せずにTclシェルモードを終了した場合、Tclシェルプロセスはアクティブなまま、対応する仮想タイプ端末VTYまたはテレタイプライタ（TTY – 回線）に接続されます。同じ回線上でデバイスにアクセスする次の認証済みユーザは、Tclシェルプロセスにアクセスし、CSCeh73049(登録ユーザのみ)またはCSCsd28570(登録ユーザのみ)と組み合わせてAAAコマンドをバイパスできます。この問題は、次のBug IDに記述されています。

- CSCef77770(登録ユーザ専用):Type ctrl-c or crtl-z causes tclsh prompt to aby

この別の問題は、次に示すIOSのバージョンにのみ存在します。

- 12.3Tベーストレイン
- 12.4ベーストレイン
- 12.2(25)S以降の列車

脆弱性が存在する製品

- Cisco IOSを実行しているすべてのシスコ製品および：
  - AAAコマンド許可機能を有効にする
  - IOSはTcl機能をサポートしています。
  - IOSバージョン12.0T以降

脆弱性が存在しない製品

- Cisco IOSを実行していない製品は影響を受けません。
- Cisco IOSバージョン12.0メインライン以前を実行している製品は該当しません。
- Cisco IOSバージョン12.0Sを実行している製品は該当しません。
- Cisco IOSを実行している製品は、AAAコマンド許可が設定されていて、Tcl機能をサポートしていない限り、この問題には該当しません。
- Cisco IOS XRを実行している製品は該当しません。

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。

ソフトウェア バージョンと修正

次の表のCisco IOSソフトウェアの各行には、リリーストレインと、対象となるプラットフォームまたは製品が記載されています。特定のリリーストレインに脆弱性が存在する場合、修正を含む最初のリリース（最初の修正リリース）とそれぞれのリリース予定日が「リビルド」列と「メンテナンス」列に表示されます。特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。このようなリリースは、少なくとも、示されているリリース以上（最初の修正リリース ラベル以上）にアップグレードしてする必要があります。

メジャー リリース	修正済みリリースの入手可能性	
該当する 12.0 ベースのリリース	リビルド	メンテナンス
12.0T	脆弱性あり、12.2(32)以降に移行	
12.0XH	脆弱性あり、12.2(32)以降に移行	
12.0XK	脆弱性あり、12.2(32)以降に移行	

12.0XL	脆弱性あり、12.2(32)以降に移行	
12.0XN	脆弱性あり、12.2(32)以降に移行	
12.0XR	脆弱性あり、12.2(32)以降に移行	
該当する 12.1 ベースのリリース	**リビルド**	**メンテナンス**
12.1	脆弱性あり、12.2(32)以降に移行	
12.1AA	脆弱性あり、12.2(32)以降に移行	
12.1E	12.1(26)E5	Â
12.1EC	脆弱性あり、12.3BC以降に移行	
12.1EZ	脆弱性あり、12.1(26)E5以降に移行	
12.1GA	脆弱性あり、12.2(32)以降に移行	
12.1GB	脆弱性あり、12.2(32)以降に移行	
12.1T	脆弱性あり、12.2(32)以降に移行	
12.1XA	脆弱性あり、12.2(32)以降に移行	
12.1XE	脆弱性あり、12.2(32)以降に移行	
12.1XH	脆弱性あり、12.2(32)以降に移行	
12.1XI	脆弱性あり、12.2(32)以降に移行	
12.1XJ	脆弱性あり、12.3(16)以降に移行	
12.1XL	脆弱性あり、12.3(16)以降に移行	
12.1XM	脆弱性あり、12.3(16)以降に移行	
12.1XP	脆弱性あり、12.3(16)以降に移行	
12.1XQ	脆弱性あり、12.3(16)以降に移行	
12.1XS	脆弱性あり、12.2(32)以降に移行	
12.1XT	脆弱性あり、12.3(16)以降に移行	
12.1XU	脆弱性あり、12.3(16)以降に移行	
12.1XV	脆弱性あり、12.3(16)以降に移行	
12.1XW	脆弱性あり、12.2(32)以降に移行	
12.1XY	脆弱性あり、12.2(32)以降に移行	
12.1XZ	脆弱性あり、12.2(32)以降に移行	
12.1YA	脆弱性あり、12.3(16)以降に移行	
12.1YB	脆弱性あり、12.3(16)以降に移行	
12.1YD	脆弱性あり、12.3(16)以降に移行	
12.1YE	脆弱性あり、12.3(16)以降に移行	
12.1YF	脆弱性あり、12.3(16)以降に移行	
12.1YH	脆弱性あり、12.3(16)以降に移行	
12.1YI	脆弱性あり、12.3(16)以降に移行	
該当する 12.2 ベースのリリース	**リビルド**	**メンテナンス**
12.2	Â	12.2(32)
12.2B	脆弱性あり。2006年4月3日に入手可能な	

	12.3(14)T7に移行してください。	
12.2BW	脆弱性あり、12.3(16)以降に移行	
12.2BY	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。	
12.2DD	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。	
12.2DX	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。	
12.2MX	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。	
12.2S	12.2(14)S16	
	12.2(18)S11	
	12.2(25)S6	
	12.2(30)Sには脆弱性があり、TACにお問い合わせください。	
12.2SU	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。	
12.2SW	12.2(25)SW5	Â
12.2SXB	12.2(17d)SXB9	Â
12.2SXD	12.2(18)SXD6	Â
12.2SXE	12.2(18)SXE3	Â
12.2SXF	脆弱性：12.2(18)SXF4への移行（2006年5月29日に入手可能）	
12.2SZ	脆弱性あり、12.2(25)S6以降に移行	
12.2T	脆弱性あり、12.3(16)以降に移行	
12.2XA	脆弱性あり、12.3(16)以降に移行	
12.2XB	脆弱性あり、12.3(16)以降に移行	
12.2XC	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。	
12.2XD	脆弱性あり、12.3(16)以降に移行	
12.2XG	脆弱性あり、12.3(16)以降に移行	
12.2XH	脆弱性あり、12.3(16)以降に移行	
12.2XJ	脆弱性あり、12.3(16)以降に移行	
12.2XK	脆弱性あり、12.3(16)以降に移行	
12.2XL	脆弱性あり、12.3(16)以降に移行	
12.2XM	脆弱性あり、12.3(16)以降に移行	
12.2XN	脆弱性あり、12.3(16)以降に移行	
12.2XQ	脆弱性あり、12.3(16)以降に移行	
12.2XS	脆弱性あり、12.3(16)以降に移行	
12.2XT	脆弱性あり、12.3(16)以降に移行	
12.2XU	脆弱性あり、12.3(16)以降に移行	
12.2XV	脆弱性あり、12.3(16)以降に移行	
12.2XW	脆弱性あり、12.3(16)以降に移行	
12.2YB	脆弱性あり、12.3(16)以降に移行	

12.2YC	脆弱性あり、12.3(16)以降に移行
12.2YD	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。
12.2YE	脆弱性あり、12.2(25)S6以降に移行
12.2YH	脆弱性あり、12.3(16)以降に移行
12.2YK	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。
12.2YL	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。
12.2YM	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。
12.2YN	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。
12.2YT	脆弱性あり、12.3(16)以降に移行
12.2YU	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。
12.2YW	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。
12.2YX	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。
12.2YY	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。
12.2YZ	脆弱性あり、12.2(25)S6以降に移行
12.2ZB	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。
12.2ZC	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。
12.2ZD	脆弱性あり。TACにお問い合わせください
12.2ZE	脆弱性あり、12.3(16)以降に移行
12.2ZF	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。
12.2ZH	脆弱性あり。TACにお問い合わせください
12.2ZJ	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。
12.2ZL	脆弱性あり。TACにお問い合わせください
12.2ZN	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。
12.2ZP	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。

該当する 12.3 ベースのリリース	**リビルド**	**メンテナンス**
12.3	Â	12.3(16)
12.3B	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。	

12.3T	12.3(11)T10（2006年3月13日に入手可能）	Â
	12.3(14)T7（2006年4月3日に入手可能）	Â
12.3XA	脆弱性あり。TACにお問い合わせください	
12.3XB	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。	
12.3XD	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。	
12.3XE	脆弱性あり。TACにお問い合わせください	
12.3XF	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。	
12.3XG	脆弱性あり。TACにお問い合わせください	
12.3XH	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。	
12.3XI	12.3(7)XI7	
12.3XJ	脆弱性あり。TACにお問い合わせください	
12.3XK	脆弱性あり。TACにお問い合わせください	
12.3XM	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。	
12.3XQ	Vulnerable; migrate to 12.4(7)、2006年3月14日より利用可能	
12.3XR	脆弱性あり。TACにお問い合わせください	
12.3XW	脆弱性あり。TACにお問い合わせください	
12.3XY	脆弱性あり。2006年4月3日に入手可能な12.3(14)T7に移行してください。	
12.3YA	C828: Vulnerable; migrate to 12.4(7)、2006年3月14日より利用可能	
	SOHO9x、C82x：脆弱性あり、TACにお問い合わせください。	
12.3YF	脆弱性あり。TACにお問い合わせください	
12.3YG	脆弱性あり。TACにお問い合わせください	
12.3YH	脆弱性あり。TACにお問い合わせください	
12.3YI	脆弱性あり。TACにお問い合わせください	
12.3YJ	脆弱性あり。TACにお問い合わせください	
12.3YK	脆弱性あり。TACにお問い合わせください	
12.3YM	12.3(14)YM6（2006年3月26日に入手可能）	Â
12.3YQ	脆弱性あり。TACにお問い合わせください	
12.3YS	脆弱性あり。TACにお問い合わせください	
12.3YT	脆弱性あり。TACにお問い合わせください	
12.3YU	脆弱性あり。TACにお問い合わせください	
12.3YX	脆弱性あり。TACにお問い合わせください	
該当する 12.4 ベー	**リビルド**	**メンテナンス**

スのリリース		
12.4	12.4(3d)（2006年3月21日に入手可能）	Â
	Â	12.4(7)（2006年3月14日に入手可能）
12.4MR	脆弱性あり。TACにお問い合わせください	
12.4T	12.4(2)T4（2006年3月20日に入手可能）	Â
	12.4(4)T2（2006年4月3日に入手可能）	Â
	Â	12.4(6)T
12.4XA	脆弱性あり。TACにお問い合わせください	
12.4XB	脆弱性あり。TACにお問い合わせください	

Â

修正済みソフトウェアの入手

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。ソフトウェアを配備する前に、メンテナンス プロバイダーと相談するか、機能セットの互換性や環境固有の既知の問題などがないかどうかを確認することを推奨いたします。

お客様は、購入した機能セットのみをインストールしてサポートを受けることができます。お客様はソフトウェア アップグレードをインストール、ダウンロード、アクセス、またはその他の方法で利用することにより、http://www.cisco.com/public/sw-license-agreement.html または http://www.cisco.com/public/sw-center/sw-usingswc.shtml に記載されている Cisco のソフトウェア ライセンス条件に同意したものと見なされます。

ソフトウェア アップグレードに関する質問は、psirt@cisco.com および security-alert@cisco.com では取り扱っていません。

サービス契約をお持ちのお客様

契約を結んでいるお客様は、定期的なアップデートチャネルを通じてソフトウェアを入手する必要があります。ほとんどのお客様は、http://www.cisco.comにあるシスコのワールドワイドWebサイトのSoftware Centerからソフトウェアパッチとバグ修正を入手できます。

サービス契約をご利用でないお客様

直接 Cisco から製品を購入し、Cisco サービス契約を結んでいないお客様や、サードパーティ ベンダーを通じて製品を購入し、そのベンダーから修正済みソフトウェアを入手できないお客様は、Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手できます。TAC の連絡先は次のとおりです。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（全世界からの有料通話）
- 電子メール：tac@cisco.com

製品のシリアル番号を入手し、ソフトウェアパッチまたはバグ修正の権利の証拠としてこの通知のURLを提供します。サービス契約を結んでいないお客様は、TACにソフトウェアパッチまたはバグ修正プログラムをリクエストする必要があります。

各国の電話番号や、各言語に対応した電子メール アドレスなど、その他の TAC 連絡先情報は、http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml を参照してください。弊社とのサポート契約がないお客様は、製品をご購入いただきました販売店経由でお問い合わせください。

サードパーティのサポート機関を利用されているお客様

Cisco パートナー、正規代理店、サービス プロバイダーなどのサードパーティ サポート機関との契約に基づいて Cisco 製品の供給および保守を受けているお客様は、このアドバイザリに関する適切な対処方法をそのサポート機関にお問い合せください。

回避策

回避策の効果は、製品の組み合わせ、ネットワークトポロジ、トラフィックの動作、組織のミッションなど、お客様の状況によって異なります。該当する製品とリリースは多岐に渡るので、サービス プロバイダーやサポート機関に連絡し、ネットワーク内で使用するのに最も適した回避策を確認してから、実際に配備することを推奨いたします。

AAA設定コマンドチェック

グローバルコンフィギュレーションコマンド**aaa authorization config-commands**を使用してIOSコンフィギュレーションコマンドの認可チェックを追加すると、AAAコマンドの認可がTclシェルモードで強制的に行われます。

注意：IOS設定コマンド許可を有効にすると、EXEC設定モード内のすべてのコマンドがコマンド許可チェックの対象になります。

AAA許可コンフィギュレーションコマンドの詳細については、http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/secur_r/sec_a1g.htm#wp1086510を参照してください。

TACACS+ユーザプロファイル内のdeny tclsh IOSコマンド

TACACS+内で定義されたすべてのユーザプロファイルにIOS EXECコマンド**tclsh**を実行する権限を与えないようにすることで、管理者はユーザが追加のコマンド特権の昇格を取得するのを防ぐことができます。ベンダーのTACACS+サーバ設定ガイドを参照して、これが正しく設定されていることを確認します。

注意：Â デバイスにアクセスできるすべてのユーザが**tclsh**コマンドにアクセスできない場合にのみ、有効な回避策となります。**tclsh**を実行するアクセス権を持ち、前述の手順では終了しない単一のユーザが、気付かないうちに、いずれかのVTYでTclシェルプロセスを実行したままにする可能性があります。

ロールベースのCLIビュー

ネットワーク管理者は、ロールベースCLIアクセス機能を使用して、「ビュー」を定義できます。ビューとは、Cisco IOS EXECおよび設定(Config)モードコマンドへの選択的または部分的なアクセスを提供する一連の操作コマンドと設定機能です。ビューは、Cisco IOSコマンドラインインターフェイス(CLI)および設定情報へのユーザアクセスを制限します。つまり、どのコマンドを受け入れ、どの設定情報を表示するかをビューで定義できます。したがって、ネットワーク管理者は、シスコのネットワークデバイスへのアクセスをより適切に制御できます。

CLIビューの詳細については、
http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part30/hclivws.htm
を参照してください。

詳細情報

Cisco IOSでは、Cisco IOSバージョン12.0(6)T以降のCisco IOS自動音声応答機能の一部として、Tool Command Language(Tcl)バージョン7.0コマンドをサポートする機能が導入されました。詳細については、
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrpg.htm を参照してください。

Tcl機能を使用したCisco IOSスクリプティングは、Tool Command Language(Tcl)バージョン8.3.4コマンドを実行する機能を提供します。これは、Cisco IOSバージョン12.3(2)Tから導入されました。詳細については、
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gt_tcl.htm
を参照してください。

シスコのセキュリティ手順

シスコ製品のセキュリティの脆弱性に関するレポート、セキュリティ障害に対する支援、およびシスコからのセキュリティ情報を受信するための登録に関するすべての情報は、シスコのワールドワイド ウェブサイト
https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html から入手できます。この情報には、シスコのセキュリティ通知に関して、報道機関が問い合せる場合の説明も含まれています。すべての Cisco セキュリティ アドバイザリは、
http://www.cisco.com/go/psirt から入手できます。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060125-aaatcl

改訂履歴

バージョン	説明	セクション	日付
Revision 2.0	2.0パブリックリリース		2006年3月1日
リビジョン1.1	ソフトウェアテーブルにリリース12.2Tを追加。		2006年1月25日
リビジョン1.0	初回公開リリース		2006年1月25日

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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。