Cisco IOSおよびIOS XEソフトウェアのTACACS+認証バイパスの脆弱性

アドバイザリーID : cisco-sa-ios-tacacs-hdB7thJw
初公開日 : 2025-09-24 16:00
バージョン 1.0 : Final
CVSSスコア : 8.1
回避策 : Yes
Cisco バグ ID : CSCwm99306

CVE-2025-20160

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 IOSソフトウェアおよびCisco IOS XEソフトウェアのTACACS+プロトコルの実装における脆弱性により、認証されていないリモートの攻撃者が機密データを表示したり、認証をバイパスしたりする可能性があります。

この脆弱性は、必要なTACACS+共有秘密が設定されているかどうかをシステムが適切にチェックしていないことに起因しています。中間者攻撃では、暗号化されていないTACACS+メッセージを傍受して読み取ったり、TACACS+サーバになりすまして任意の認証要求を不正に受け入れたりすることで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は、TACACS+メッセージの機密情報を表示したり、認証をバイパスして該当デバイスにアクセスしたりできる可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。本脆弱性に対処する回避策がいくつかあります。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-tacacs-hdB7thJw

このアドバイザリは、Cisco IOSおよびIOS XEソフトウェアのセキュリティアドバイザリバンドル公開の2025年9月リリースの一部です。これらのアドバイザリとリンクの一覧については、『シスコイベントレスポンス：Cisco IOSおよびIOS XEソフトウェアに関するセキュリティアドバイザリ公開資料（半年刊、2025年9月）』を参照してください。

該当製品

脆弱性のある製品

この脆弱性は、Cisco IOSおよびIOS XEソフトウェアの脆弱性が存在するリリースを実行し、TACACS+を使用するように設定されているがTACACS+共有秘密が欠落しているシスコデバイスに影響を与えます。

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

デバイス設定の確認

デバイスでTACACS+またはTACACS+サーバの共有秘密が設定されているかどうかを確認するには、次の項の手順を使用します。

TACACS+設定の確認

デバイスでTACACS+が設定されているかどうかを確認するには、show running-config | include tacacs CLIコマンドまたはshow running-config | section tacacs CLIコマンドを使用します。出力されない場合、デバイスはこの脆弱性の影響を受けません。出力がある場合は、TACACS+が設定されており、デバイスが影響を受ける可能性があります。

次の例は、グループが設定されているデバイスの出力を示しています。

<#root>

```
Router#
show running-config | include tacacs


aaa group server tacacs+ ise1
tacacs server ise
```

次の例は、グループが設定されていないデバイスの出力を示しています。

<#root>

```
Router#
show running-config | section tacacs


address ipv4 10.1.1.1
tacacs-server key cisco123
Router#
```

次の例は、server-privateが設定されているデバイスでの出力を示しています。

```
<#root>

Router#

show running-config | section tacacs


aaa group server tacacs+ ise
 server-private 10.1.1.1
tacacs server ise
 address ipv4 10.1.1.1
 key Cisc0123
```

TACACS+サーバキー設定の確認

デバイスにTACACS+サーバ共有秘密が設定されているかどうかを確認するには、show running-config | include tacacs server|key CLIコマンドを使用します。設定されているすべてのTACACS+サーバに共有秘密が設定されている場合、そのデバイスは影響を受けません。いずれかの TACACS+サーバが共有キーなしで設定されている場合、そのデバイスは影響を受けます。

次の例は、Groupsが設定されている、Groupsが設定されていない、またはserver-privateが設定されている該当デバイスからの出力を示しています。欠落しているキー行に注意してください。

```
<#root>

Router#

show running-config | include tacacs server|key

tacacs server ise
```

次の例は、該当せず、Groupsが設定されている、Groupsが設定されていない、またはserver-privateが設定されているデバイスからの出力を示しています。キーcisc0123の共有秘密を確認します。

```
<#root>

Router#

show running-config | include tacacs server|key

tacacs server ise
```

```
key cisco123
```

注：各TACACS+サーバでは、影響を受けないようにキーを設定する必要があります。

次の例は、複数のTACACS+サーバが設定されている該当デバイスからの出力を示しています。ise2の欠落しているキー行に注意してください。

```
<#root>

Router#

show running-config | include tacacs server|key

tacacs server ise1
 key cisco123
tacacs server ise2
```

次の例は、複数のTACACS+サーバが設定されている、該当しないデバイスからの出力を示しています。両方のTACACS+サーバのキーcisc0123の共有秘密に注意してください。

```
<#root>

Router#

show running-config | include tacacs server|key

tacacs server ise1

key cisco123

tacacs server ise2

 key cisco123
```

次の例は、グローバルに設定されたTACACS+キーを持つ複数のTACACS+サーバがある、該当しないデバイスからの出力を示しています。 key cisc0123 shared secretがグローバルに設定されている点に注意してください。

```
<#root>

Router#

show running-config | include tacacs server|key
 tacacs server key 7 cisco123


tacacs server ise1
```

```
tacacs server ise2
```

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションにリストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- IOS XR ソフトウェア
- NX-OS ソフトウェア

回避策

この脆弱性に対処する回避策はありません。デバイスに設定されているすべてのTACACS+サーバに共有秘密が設定されていることを確認します。

この回避策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

修正済みソフトウェア

シスコでは、修正済みソフトウェアリリースへのアップグレードが利用可能になるまで、回避策や緩和策は一時的な解決策であると考えています。この脆弱性を完全に修復し、本アドバイザリで説明されている障害の発生を回避するために、お客様には本アドバイザリで説明されている修正済みソフトウェアにアップグレードすることを強く推奨します。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS および IOS XE ソフトウェアの脆弱性による侵害の可能性を判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。あるいは、次のフォームを使用して、シスコ セキュリティ アドバイザリに該当するリリースであるかどうかを確認します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. リリース番号（例：15.9(3)M2、17.3.3）を入力します。
3. [チェック（Check）] をクリックします。

2 | | Critical,High,Medium
このアドバイザのみ

Enter release number | Check

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

出典

この脆弱性は、Cisco Technical Assistance Center(TAC)のサポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-tacacs-hdB7thJw

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2025年9月24日

利用規約

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。