Cisco IOS および IOS XE ソフトウェアのコマンドにおける許可バイパスの脆弱性

アドバイザリーID : cisco-sa-aaascp-Tyj4fEJm
初公開日 : 2023-09-27 16:00
最終更新日 : 2023-10-13 13:36
バージョン 1.1 : Final
CVSSスコア : 8.0
回避策 : Yes
Cisco バグ ID : CSCwe55871

CVE-2023-20186

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 ソフトウェアの認証、許可、およびアカウンティング（AAA）機能における脆弱性により、認証されたリモート攻撃者が、コマンド許可をバイパスし、Secure Copy Protocol（SCP）を使用して該当デバイスのファイルシステムに、またはファイルシステムから、ファイルをコピーする可能性があります。

この脆弱性は、AAA コマンド許可チェックでの SCP コマンドの不適切な処理に起因します。有効なログイン情報を持つ特権レベル 15 の攻撃者は、SCP を使用して外部マシンから該当デバイスに接続することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者が該当デバイスの設定を取得または変更し、該当デバイスにファイルを配置したり、該当デバイスからファイルを取得したりす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-aaascp-Tyj4fEJm

このアドバイザリは、2023 年 9 月に公開された Cisco IOS および IOS XE ソフトウェア セキュリティ アドバイザリ バンドルの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: September 2023 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication』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 ソフトウェアまたは Cisco IOS XE ソフトウェアの脆弱性のあるリリースを自律モードまたはコントローラモードで実行しており、SCP サーバー機能と AAA コマンド許可の両方が有効になっているシスコ製品に影響を与えます。ただし、デバイスがエクスプロイト可能かどうかは、各ユーザーの TACACS+ プロファイルの設定方法によって異なります。詳細については、このアドバイザリの「詳細情報」のセクションを参照してください。

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。

SCP サーバー設定の確認

SCP サーバーを有効にするようにデバイスが設定されているかどうかを確認するには、そのデバイスにログインし、CLI で show running-config | include ip scp server enable コマンドを使用します。SCP サーバーを有効にするようにデバイスが設定されている場合は、次の例のように、出力に ip scp server enable コマンドが含まれます。

```
<#root>

Router#

show running-config | include ip scp server enable

ip scp server enable
Router#
```

show running-config | include ip scp server enable コマンドを実行しても出力が返されない場合、デバイスは SCP サーバーを有効にするように設定されていません。

AAA 設定の確認

デバイスがログイン許可に AAA を使用するよう設定されているかどうかを確認するには、そのデバイスにログインし、CLI で show running-config | include aaa authorization commands コマンドを使用します。次の例のように、コマンドを実行して何らかの出力が返される場合、そのデバイスは AAA コマンド許可を使用するように設定されています。

```
<#root>

Router#

show running-config | include aaa authorization commands
```

```
aaa authorization commands 15 ISE_aaa group ISESERVER local
Router#
```

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記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

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
- Meraki 製品
- NX-OS ソフトウェア

詳細

SCP サーバーが有効になっている場合、適切な許可を得たユーザーは、イメージや設定を含む任意のファイルを Cisco IOS ファイルシステムに、またはファイルシステムから、コピーできます。特権レベル 15 が割り当てられたユーザーだけが SCP サーバーを使用できます。管理者は、コマンド許可を適用することで、認証されたユーザーが実行できるアクションをさらに制限できます。コマンド許可は、特権レベルごとに適用されます。

この脆弱性によって受ける影響は、特権レベル 15 のユーザーに関するポリシーがどのように定義されているかによって異なります。特権レベル 15 のユーザーが設定を表示または変更できないという制限がデバイスにある場合、ユーザーは、SCP によって設定を取得し、ローカルで設定を変更してから、SCP によってその設定をコピーしてデバイスに戻すことで、設定を変更できます。

AAA コマンド許可が有効になっている場合、SCP ユーザーが特権レベル 15 のユーザーである必要があるとすると、SCP コマンドは設定行 aaa authorization commands 15 で処理される必要があります。ただし、この脆弱性により、要求が代わりに設定行 aaa authorization commands 0 によって処理されます。

SCP クライアント機能は影響を受けません。

SSH サーバーおよびクライアント機能は影響を受けません。

回避策

この脆弱性に対処する回避策と軽減策があります。

この脆弱性の回避策としては、特権レベル 0 コマンド許可チェックを有効にします。AAA サーバーに SCP サーバーコマンドを強制的にチェックさせるには、設定コマンド aaa authorization

commands 0 を使用し、ユーザーが SCP サーバーコマンドを使用できないようにする適切なコマンドポリシーを設定します。SCP によるファイルのアップロードやダウンロードを許可または拒否するには、コマンド scp -f および scp -t の AAA 設定にフィルタを追加します。

この脆弱性の緩和策としては、設定コマンド no ip scp server enable を使用して SCP サーバー機能を無効にします。その後、管理者は、該当デバイスで SCP クライアント機能を使用して、イメージや設定をルータに、またはルータから、コピーできます。

この回避策と緩和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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのような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使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレード ソリューション一式を確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に

確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS ソフトウェアおよび 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（15.9(3)M2、17.3.3 など）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

この脆弱性を報告していただいた Hendrik Van Belleghem 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aaascp-Tyj4fEJm

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	属性を追加。	出典	Final	2023 年 10 月 13 日
1.0	初回公開リリース	—	Final	2023 年 9 月 27 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。