Cisco IOS XE ソフトウェアの静的クレデンシャルの脆弱性

Critical

アドバイザリーID : cisco-sa-20180328-xesc

初公開日 : 2018-03-28 16:00

最終更新日 : 2018-09-19 16:00

バージョン 2.0 : Final

CVSSスコア : 9.8

回避策 : Yes

Cisco バグ ID : CSCve89880 CSCve76719

CVE-2018-0150

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 XE ソフトウェアの脆弱性により、認証されていないリモート攻撃者が、影響を受ける Cisco IOS XE ソフトウェア リリースを実行しているデバイスに、初期ブート時に使用されるデフォルトのユーザ名とパスワードでログインできる可能性があります。

この脆弱性は、権限レベル 15 の未公開のユーザ アカウントにデフォルトのユーザ名とパスワードが設定されていることに起因します。 攻撃者は、このアカウントを使用してリモートから該当デバイスに接続することにで、本脆弱性を不正利用する可能性があります。 攻撃者が不正利用に成功すると、レベル 15 のアクセス権限でデバイスにログインできる可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-xesc
このアドバイザリは、2018 年 3 月 28 日 発行の Cisco IOS および IOS XE ソフトウェア Security Advisory Bundled Publication の一部であり、22 の脆弱性を説明する 20 のシスコ セキュリティ アドバイザリが含まれています これらのアドバイザリとリンクの一覧については、以下を参照してください。Cisco Event Response: March 2018 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication。

該当製品

脆弱性のある製品

この脆弱性は、脆弱性が存在する Cisco IOS XE ソフトウェア リリースを実行しているシスコ デバイスに影響を及ぼします。

- Cisco bug CSCve89880 の対象は、Cisco IOS XE ソフトウェア リリース 16.5 トレインまたはそれ以降のトレインを実行しているデバイスです。 この脆弱性は、ソフトウェア リリース 16.5.2 以降、およびリリース 16.6.1 以降で修正されています。
- Cisco bug CSCve76719 の対象は、Cisco 統合サービス仮想ルータ（ISRv）で実行されている Cisco IOS XE ソフトウェア リリースです。 脆弱性が存在するソフトウェア 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」の項を参照してください。

本脆弱性は、リリース 16.x より前の Cisco IOS XE ソフトウェア リリースには影響を与えません。

Cisco IOS XE ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS XE ソフトウェア リリースは、管理者がデバイスにログインして、CLI で **show version コマンド**を実行し、表示されるシステム バナーを参照することにより確認できます。 デバイスが Cisco IOS XE ソフトウェアを実行している場合、システム バナーに「*Cisco IOS Software*」、「*Cisco IOS XE Software*」などのテキストが表示されます。

次に、Cisco IOS XR ソフトウェア リリース 16.2.1 が実行されていて、インストールされているイメージ名が *CAT3K_CAA-UNIVERSALK9-M* であるデバイスでのコマンドの出力例を示します。

```
ios-xe-device# show version

Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali
16.2.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 by mcpre
.
.
.
```

Cisco IOS XE ソフトウェア リリースの命名と番号付けの規則に関する詳細は、『Cisco IOS and NX-OS Software Reference Guide』を参照してください。

脆弱性を含んでいないことが確認された製品

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。

シスコは、この脆弱性が Cisco IOS ソフトウェア、Cisco IOS XR ソフトウェア、および Cisco

NX-OS ソフトウェアには影響を与えないことを確認しました。

回避策

本脆弱性に対処するために、管理者はデバイス設定で **no username cisco** コマンドを使用してデフォルト アカウントを削除できます。 また、デバイスにログインして、このアカウントのパスワードを変更することでも対処できます。

Cisco ISRv について、管理者はデータストアから古いパッケージを削除し、ISRv パッケージを更新して、新たに導入された Cisco ISRv にデフォルトのアカウントが含まれないようにする必要があります。

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 アップデートを提供しています。 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts 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完全なアップグレード ソリューション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 に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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

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、シスコでは Cisco IOS Software Checker ツールを提供しています。このツールにより、特定のソフトウェア リリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。 また該当する場合、すべてのアドバイザリに記載された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。

このツールを使用して次のタスクを実行できます。

- ドロップダウン リストからリリース（複数可）を選択するか、分析対象となるローカル システムからファイルをアップロードして、検索を開始する
- **show version** コマンドの出力をツールで解析する
- カスタマイズした検索（過去に公開されたすべてのシスコ セキュリティ アドバイザリを検索対象に含めたり、特定のアドバイザリのみ、または最新のバンドル資料から全アドバイザリを含めるなど）を作成する

リリースが、公開されたシスコ セキュリティ アドバイザリのいずれかに該当するかどうかを確認するには、Cisco.com の Cisco IOS Software Checker を使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェア リリース（たとえば、**15.1(4)M2**、**3.13.8S** など）を入力します。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-xesc

改訂履歴

Version	Description	Section	Status	日付
2.0	Cisco ISRv が影響を受け、別のコード修正があるということが明記されています。	「脆弱性のある製品」、「回避策」	Final	2018

				年 9 月 19 日
1.0	初回公開リリース		Fin al	20 18 年 3 月 28 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。