

Cisco IOS XE ソフトウェアのコマンド インジェクションの脆弱性



アドバイザリーID : cisco-sa-20180926-

iosxe-cmdinj

初公開日 : 2018-09-26 16:00

バージョン 1.0 : Final

CVSSスコア : [6.7](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvh02919](#) [CSCvh54202](#)

[CVE-2018-](#)

[0481](#)

[CVE-2018-](#)

[0477](#)

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 CLI パーサーにおける複数の脆弱性により、認証されたローカル攻撃者が影響を受けるデバイスの基盤となる Linux シェルで、ルート権限を使用して任意のコマンドを実行できる可能性があります。

この脆弱性は、影響を受けるソフトウェアのコマンド引数のサニタイズが不適切なために、影響を受けるデバイスの特定の内部データ構造へのアクセス防止に失敗することで発生します。攻撃者が影響を受けるデバイスに特権 EXEC モード (特権レベル 15) でアクセスできる場合、カスタム引数を含む CLI コマンドを実行することで、デバイス上でこれらの脆弱性をエクスプロイトする可能性があります。エクスプロイトが成功すると、該当デバイスで、任意のコマンドが root 権限で実行される可能性があります。

シスコはこれら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。これらの脆弱性に対処する回避策はありません。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-iosxe-cmdinj>

このアドバイザリーは、2018 年 9 月 26 日に公開された 13 件の脆弱性に関する 12 件のシスコ セキュリティ アドバイザリーを含む Cisco IOS ソフトウェアおよび IOS XE ソフトウェア リリースのセキュリティ アドバイザリー公開資料の一部です。アドバイザリーとリンクの一覧については、『[Cisco Event Response: September 2018 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 XE ソフトウェアの脆弱性が存在するリリースを実行しているシステムデバイスに影響を及ぼします。

脆弱性が存在する Cisco IOS XE 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。

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。

```
<#root>
```

```
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

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、これら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 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

これらの脆弱性に対処する回避策はありません。

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。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です。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、[シスコのセキュリティアドバイザリおよびアラート (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 Cisco Service Contract 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 POS 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

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するため、シスコは Cisco IOS Software Checker ツールを提供しています。このツールを使用すると、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、そのリリースに関するすべてのアドバイザリ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入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべての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または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。

<input type="text"/>	<input type="button" value="Check"/>
----------------------	--------------------------------------

デフォルトでは、Cisco IOS ソフトウェアのチェックには、結果は、高セキュリティへの影響の評価 (サー) または重大な脆弱性にのみが含まれています。「中間」の SIR 脆弱性の結果を含めるには、Cisco.com の Cisco IOS ソフトウェア チェッカーを使用して、[Impact Rating] ドロップダウン リストの [中間 (Medium)] チェックボックスをオンにします。

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、Cisco IOS XE ソフトウェアのリリースに応じて「[Cisco IOS XE 2 Release Notes](#)」、「[Cisco IOS XE 3S Release Notes](#)」、または「[Cisco IOS XE 3SG Release Notes](#)」を参照してください。

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とその公表は確認しておりません。

出典

この脆弱性は、シスコ内部でのシステム セキュリティ テストによって発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa->

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	2018年9月26日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、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。