Cisco IOS XEソフトウェアのディレクトリトラバーサルの脆弱性

Medium

アドバイザリーID : cisco-sa-20161115-iosxe　CVE-2016-6450
初公開日 : 2016-11-15 16:00
バージョン 1.0 : Final
CVSSスコア : 1.5
回避策 : No workarounds available
Cisco バグ ID : CSCva60013 CSCvb22622

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 package unbundleユーティリティにおける脆弱性により、認証されたローカル攻撃者が、基盤となるオペレーティングシステムの一部のファイルに対する書き込みアクセス権を取得する可能性があります。

この脆弱性は、該当するインストールユーティリティに送信されたファイルの検証が不十分であることに起因します。攻撃者は、巧妙に細工されたファイルを該当システムにアップロードし、インストールユーティリティコマンドを実行することで、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、攻撃者は基盤となるオペレーティングシステムの一部のファイルに書き込みアクセス権を取得し、書き込みアクセス可能なファイルを上書きしてシステムの整合性を損なう可能性があります。

この脆弱性を不正利用するには、攻撃者は適切なコマンドを実行するための十分な権限を持っている必要があります。デフォルト設定では、この脆弱性を不正利用するために privilege 15権限が必要です。この脆弱性の二次的な影響として、攻撃者は有効なライセンスを提供しなくても、一部のファイルを変更して、基盤となるオペレーティングシステムシェルにアクセスできる可能性があります。

こ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-20161115-iosxe

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次の製品に影響を与えます。

- Cisco 5700 シリーズ ワイヤレス LAN コントローラ
- Cisco Catalyst 3650 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 4500Eシリーズスイッチ
- Cisco Catalyst 4500Xシリーズスイッチ

この脆弱性は設定固有のものではありません。上記の製品はすべて、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場合に脆弱になります。脆弱性のあるソフトウェアリリースの詳細については、このアドバイザリの冒頭にあるCisco Bug IDを参照してください。

この脆弱性を工クスプロイトするには、攻撃者が該当システムへの特権アクセス権を持ち、巧妙に細工されたファイルを転送してシステム上で特権コマンドを実行できる必要があります。

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、コマンドラインインターフェイス(CLI)で show versionコマンドを使用し、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 XE Software」などのテキストが表示されます。

次に、Cisco IOS XEソフトウェアリリース3.6.5Eを実行しているデバイスでの show versionコマンドの出力例を示します。

<#root>

```
Router>

show version


Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Thu 02-Jun-16 09:03 by prod_rel_team
.
.
.
```

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、『 White

Paper: 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。

回避策

こ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

修正済みソフトウェアリリースの詳細については、このアドバイザリの冒頭にあるCisco Bug IDを参照してください。

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。

推奨事項

$propertyAndFields.get("recommendations")

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、Digital Security Ltd.のMaksim Malyutin氏によってシスコに報告されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161115-iosxe

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	2016年11月15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。