Cisco IOS XE ソフトウェア ギガビット イーサネット（802.3z）マネージメントインターフェイス アクセス制御リスト バイパスの脆弱性

Medium	**アドバイザリーID :** cisco-sa-20190327-mgmtacl **初公開日 :** 2019-03-27 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 5.3 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvm97704 CSCvk47405	CVE-2019-1759

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 ソフトウェアのリモート攻撃者 マネージメントインターフェイス ギガビット イーサネット（802.3z）マネージメントインターフェイスの Access Control List （ ACL ） 機能の脆弱性は非認証がの設定された IP アドレスにギガビット イーサネット（802.3z）達するようにする可能性があります。

脆弱性は Cisco IOS XE ソフトウェア 16.1.1 リリースでもたらされた論理エラーが原因です、マネージメントインターフェイスに対して適用されたとき ACL ははたらくことを防ぐ。 攻撃者はマネージメントインターフェイスによってデバイスにアクセスするように試みによってこの問題を不正利用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ました。 この脆弱性に対処する部分的な回避策があります。

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-20190327-mgmtacl

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 な 16.x リリースを実行して、マネージメントインターフェイスの Access Control List （ ACL ）でギガビット イーサネット（ 802.3z ）設定される Ciscoデバイスに影響を与えます。 本脆弱性は、Cisco IOS XE リリース 16.1.1 で取り込まれました。

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。

マネージメントインターフェイスをギガビット イーサネット (802.3z) 査定すること

、管理者はデバイスにログイン ギガビット イーサネット（ 802.3z ） マネージメントインターフェイス 設定が影響を受けているかどうか判別し、**show running-config を**使用するためにできます **| ip access-group コマンド**または **IPv6 トラフィック フィルタ** コマンドの存在があるように確認するべき CLI の**セクション インターフェイス GigabitEthernet0$** コマンド。 どちらかのコマンドがおよび設定されてある場合、デバイスに影響を受けた設定があります。

次に、 IPv4 ヘルパー アドレスが設定されたデバイス上の **show running-config |** 影響を受けた設定があるルータのための**セクション インターフェイス GigabitEthernet0$** コマンド:

```
Router# sh running-config | section interface GigabitEthernet0$
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 ip address 192.168.1.1 255.255.255.0
 ip access-group 100 in
```

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

このアドバイザリの脆弱性が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

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。

詳細

アクセス リストがマネージメントインターフェイスにギガビット イーサネット (802.3z) 追加される場合、バイパスされる ACL に終って Cisco IOS XE ソフトウェア リリース 16.1.1 からまで最初の修正、評価されません。

すべてのプラットフォームは Cisco バグ ID CSCvm97704 の下で当たる Cisco Catalyst 9200 シリーズ スイッチを除いて Cisco バグ ID CSCvk47405 の下で当たります。

回避策

TTY を活用 する 機能の場合、管理者は次の例に示すようにそれらのアプリケーションのためのこの脆弱性を軽減するすべての VTY 行にアクセス制御リストを適用できます:

```
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
.
.
.
```

デバイスでアクセス可能であるが、使用しませんアプリケーションは (サポートされるところ) アプリケーション固有 ACL が設定されなければならない TTY を。 1 つの例は HTTPサーバが有効に なる場合です。 HTTPサーバ ACL を適用するために、次の例を参照して下さい:

```
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
```

.
.
.
デバイスでアクセス可能であるアプリケーションはまだ TTY が割り当てられるように要求しないアプリケーション固有 ACL を露出されますサポートしないし。 2 つの例は TFTP および FTP です。

修正済みソフトウェア

影響を受けたおよび修正済みソフトウェアリリースについての詳細な情報に関しては、Cisco IOSソフトウェア チェッカーを参照して下さい。

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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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。

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、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

リリースがあらゆる公開された Cisco Security Advisory から影響を受けするかどうか判別するために、Cisco.com の Cisco IOSソフトウェア チェッカーを使用するか、または—次のフィールドで… Cisco IOS か IOS XE ソフトウェア リリースを—たとえば、**15.1(4)M2** か **3.13.8S** 入力して下さい:

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やその公表を確認していません。

出典

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

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-mgmtacl

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019 年 3 月 27 日

利用規約