Cisco Industrial Ethernetシリーズスイッチの Cisco IOSソフトウェアにおけるアクセスコントロールリストバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-repacl-9eXgnBpD
初公開日 : 2024-09-25 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : No workarounds available
Cisco バグ ID : CSCwi85609

CVE-2024-20465

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 Industrial Ethernet 4000、4010、および5000シリーズスイッチで実行されているCisco IOSソフトウェアのアクセスコントロールリスト(ACL)プログラミングの脆弱性により、認証されていないリモートの攻撃者が設定されたACLをバイパスできる可能性があります。

この脆弱性は、管理者がResilient Ethernet Protocol(REP)を有効または無効にする際に、スイッチ仮想インターフェイスでIPv4 ACLが正しく処理されないことに起因します。攻撃者は、該当デバイスを介してトラフィックを送信しようとすることで、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、攻撃者は該当デバイスのACLをバイパスでき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。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-repacl-9eXgnBpD

このアドバイザリは、Cisco IOSソフトウェアおよびIOS XEソフトウェアのセキュリティアドバイザリバンドル公開の2024年9月リリースの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: September 2024 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

公開時点では、次のシスコ製品でCisco IOSソフトウェアリリース15.2(8)E2以降が実行されており、スイッチ仮想インターフェイス(SVI)にIPv4 ACLが設定されている場合、この脆弱性の影響を受けます。

- Industrial Ethernet 4000 シリーズ スイッチ
- Industrial Ethernet 4010 シリーズ スイッチ
- Industrial Ethernet 5000 シリーズ スイッチ

デバイス設定の確認

デバイスでSVIにIPv4 ACLが設定されているかどうかを確認するには、show running-config | begin ^interface Vlan CLIコマンドを使用します。次の例に示すように、各SVI(インターフェイスVlan x)の下の内容を調べて、IPv4アクセスグループが設定されているかどうかを確認します。

<#root>

```
Switch#
show running-config | begin ^interface Vlan


interface Vlan 100


 ip address 192.168.1.1 255.255.255.0


ip access-group
DropACL in
Switch#
```

注：この脆弱性は、管理者がアップリンクインターフェイスでREPを有効または無効にした場合にのみエクスプロイト可能になります。脆弱性のある状態でACLが評価されていない場合は、回復するためにデバイスをリロードし、ACLが正しく機能していることを確認します。

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 XE ソフトウェア
- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア

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

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。

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

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-repacl-9eXgnBpD

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	2024年9月25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。