Cisco IOS XEソフトウェアのNETCONF/RESTCONF IPv4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-dmi-acl-bypass-Xv8FO8Vz
初公開日 : 2024-03-27 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : Yes
Cisco バグ ID : CSCwe12169 CSCwf92391

CVE-2024-20316

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ソフトウェアのデータモデルインターフェイス(DMI)サービスの脆弱性により、認証されていないリモートの攻撃者が、設定済みのIPv4アクセスコントロールリスト(ACL)で保護されているはずのリソースにアクセスできる可能性があります。

この脆弱性は、正常に認証されたデバイス管理者がNETCONFまたはRESTCONFプロトコルを使用してIPv4 ACLを更新し、更新されたACLのアクセスコントロールエントリ(ACE)を並べ替える際のエラー状態の不適切な処理に起因します。攻撃者は、影響を受けるデバイスで保護されているべきリソースにアクセスすることで、この脆弱性を不正利用する可能性があります。

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。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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dmi-acl-bypass-Xv8FO8Vz

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3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: March 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

この脆弱性の公開時点では、シスコデバイスで脆弱性が存在するCisco IOS XEソフトウェアリリースを実行していて、設定済みのIPv4 ACLを管理するためにNETCONFまたはRESTCONF機能を有効にしている場合に、シスコデバイスに影響が及びました。

次のACLタイプがこの脆弱性の影響を受けます。

- IPv4標準ACL
- logまたはlog-inputオプション付きのACEが含まれている場合のIPv4拡張ACL

IPv6 ACLは、この脆弱性の影響を受けません。

脆弱性が存在する Cisco 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。

デバイス設定の確認

Cisco IOS XEソフトウェアでは、NETCONFとRESTCONFの両方の機能がデフォルトで無効になっています。

NETCONFが有効になっているかどうかの確認

Netconf機能が有効になっているかどうかを確認するには、show running-config | include netconf-yang CLIコマンドを使用します。コマンドの出力自体が1行でnetconf-yangを返す場合、次の例に示すように、NETCONF機能が有効になっています。

<#root>

```
router#
```

show running-config | include netconf-yang

netconf-yang

```
netconf-yang feature candidate-datastore
router#
```

このコマンドの出力が空の場合、または単独でnetconf-yangが回線に含まれていない場合、NETCONF機能は無効になります。

RESTCONFが有効になっているかどうかの確認

RESTCONF機能が有効になっているかどうかを確認するには、show running-config | include

restconf CLIコマンドを使用します。コマンドの出力自体が1行でrestconfを返す場合は、次の例に示すように、RESTCONF機能が有効になっています。

```
<#root>

router#

show running-config | include restconf


restconf


router#
```

このコマンドの出力が空の場合、または単独でrestconfが行に含まれていない場合、RESTCONF機能は無効になります。

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 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

セキュリティ侵害の痕跡

デバイスログに次のメッセージが記録されている場合、デバイスは脆弱な状態にある可能性があります。

```
%DMI-5-SYNC_NEEDED: RO/O: dmiauthd: Configuration change requiring running configuration sync detected
%DMI-5-SYNC_START: RO/O: dmiauthd: Synchronization of the running configuration to the NETCONF running
%DMI-3-SYNC_ERR: RO/O: dmiauthd: An attempt to synchronize the running configuration to the NETCONF run
%DMI-3-DMI_DEGRADED: RO/O: dmiauthd: The dmi infra is operating in degraded mode.  Most synchronization
```

デバイスでこれらのログが見られる場合、特に設定されたACLに関して、現在のrunning-configとデバイスの予想される設定を手動で比較します。

回避策

この脆弱性に対処する回避策はありません。

NETCONFまたはRESTCONFプロトコルを使用する代わりに、デバイスCLIで直接ACLを管理します。

この回避策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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	オン	

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

この脆弱性を報告していただいたTronet社のAndrej Mikus氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dmi-acl-bypass-Xv8FO8Vz

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3月27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。