Cisco IOS XRソフトウェアのモデル駆動型プログラマビリティの動作とAAA認可

アドバイザリーID : cisco-sa-iosxr-info-GXp7nVcP
初公開日 : 2023-09-13 16:00
バージョン 1.0 : Final
回避策 : Yes
Cisco バグ ID :

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 XRソフトウェアは、データモデルを使用してネットワークデバイスの運用データをプログラムによって設定および収集する方法をサポートしています。データモデルは、NETCONFまたはgRPCを使用してネットワーク内のデバイスの機能へのアクセスを提供します。

Cisco IOS XRソフトウェアのコンフィギュレーションガイドによると、デバイスでNETCONFまたはgRPCが有効になっている場合は、不正アクセスを防ぐために認証、許可、アカウンティング(AAA)許可を設定する必要があります。

AAA認可を設定して、ユーザのアクセスを制御されないように制限します。AAA認可が設定されていない場合、ユーザに割り当てられたグループに関連付けられたコマンドとデータルールはバイパスされます。IOS-XRユーザは、Network Configuration Protocol(NETCONF)、google定義のRemote Procedure Calls(gRPC)、または任意のYANGベースのエージェントを使用して、IOS-XR設定に対する完全な読み取り/書き込みアクセスを持つことができます。非制御アクセスの許可を回避するには、設定をセットアップする前に、aaa authorization execコマンドを使用してAAA認可を有効にします

この情報アドバイザリでは、NETCONFまたはgRPC（gRPCネットワーク管理インターフェイスまたはgRPCネットワーク操作インターフェイス）が設定されている場合に、デバイスにAAA認証が設定されていないことによる影響について説明します。

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-iosxr-info-GXp7nVcP

このアドバイザリは、2023年9月に公開されたCisco IOS XRソフトウェアセキュリティアドバイ

ザリバンドルの一部です。これらのアドバイザリとそのリンクの一覧については、『Cisco Event Response: September 2023 Semiannual Cisco IOS XR Software Security Advisory Bundled Publication』を参照してください。

脆弱性のある製品

この情報アドバイザリは、Cisco IOS XRソフトウェア(CatOS)およびCisco IOS XR7(LNT)がNETCONFまたはgRPCをサポートし、これらを使用して設定されている場合に適用されます。AAAが有効になっていない場合、タスクベースのアクセス制御は適用されません。

NETCONFとgRPCが設定されているかどうかの確認

Cisco IOS XRソフトウェアを実行しているデバイスが、NETCONFまたはgRPCのいずれかを使用するように設定されているかどうかを確認するには、show running-config netconf-yang agentおよびshow running-config grpc CLIコマンドを使用します。次の例に示すように、どちらかのコマンドが出力を返すと、対応するプロトコルが有効になります。

```
<#root>

RP/0/RP0/CPU0:8101-A#

show running-config netconf-yang agent

Sun Mar  5 23:18:28.756 UTC
netconf-yang agent
 ssh
!

RP/0/RP0/CPU0:8101-A#

show running-config grpc

Sun Mar  5 23:18:38.070 UTC
grpc
 port 57400
!

RP/0/RP0/CPU0:8101-A#
```

AAA認可EXECが設定されているかどうかの確認

Cisco IOS XRソフトウェアを実行しているデバイスにAAA認可EXECが設定されているかどうかを確認するには、show running-config aaa authorization CLIコマンドを使用します。次の例に示すような出力がコマンドから返された場合は、AAA認可EXECが有効になっています（この場合はデフォルトメソッドが使用されています）。

```
<#root>
```

```
RP/0/RSP0/CPU0:SR1#

show running-config aaa authorization

Sun Mar  5 23:44:05.479 UTC
aaa authorization exec default local

RP/0/RSP0/CPU0:SR1#
```

AAA認可EXECがデバイスで設定されていないが、NETCONF、gRPC、またはその両方がデバイスで設定されている場合は、影響があります。これらの影響の詳細については、このアドバイザリの「詳細」セクションを参照してください。

注： NETCONFは、aaa authorization nacm CLIコマンドを使用して設定されるNETCONF Access Control Model(NACM)をサポートしています。デバイスでNETCONFとNACMの両方の認可が有効で、gRPCが有効になっていない場合、このアドバイザリで説明されている問題に対処するためにAAA認可EXECは必要ありません。

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 XE ソフトウェア
- NX-OS ソフトウェア

詳細

シスコでは、NETCONFまたはgRPCを使用している場合はAAA設定を確認し、このアドバイザリに記載されているセキュリティの問題を回避するようにAAA認可EXECが設定されていることを確認することをお勧めします。

NETCONFの動作

クライアントは、NETCONFエージェントへのSSHを介してNETCONFセッションを確立します。AAA認可EXECが設定されている場合、設定された方式リストが返されます。AAA認可EXECが設定されていない場合は、デフォルトの方式リストが返されます。

Cisco IOS XR7(LNT)では、AAA許可EXECが設定されていない場合、許可はスキップされます。この問題は、Cisco Bug CSCwe35622で対処されています。

次の表に、NETCONFを使用したタスクベースの認証適用の概要を示します。

Cisco IOS XR ソフトウェア	タスクベースの承認は適用されますか。				
	AAAなし	AAAログイン認証を使用し、AAA認可EXECを使用しない場合	AAA認可EXECを使用する場合	デフォルトのNACM	設定済みのNACMを使用
Cisco IOS XR（32ビット）	強制されません。	強制されません。	強制：	強制：	強制：
Cisco IOS XR（64ビット）	リリース7.1.1以前：適用されません。 リリース7.1.2以降：適用。	リリース7.1.1以前：適用されません。 リリース7.1.2以降：適用。	強制：	強制：	強制：
Cisco IOS XR7(LNT)	強制されません。CSCwe35622による修正が必要です。	強制されません。CSCwe35622による修正が必要です。	強制：	強制：	強制：

注： NETCONFでサポートされるのはデフォルトの方式リストだけです。したがって、お客様は使用しているデバイスでaaa authorization exec default <method>が設定されていることを確認する必要があります。

gRPCの動作

クライアントは、Cisco IOS XRソフトウェアのmgbl Extensible Manageability Services(EMSd)プロセスを介してgRPCセッションを確立し、YANGフレームワーク(YFW)エンコード/デコード層に渡されます。EMSdはYFWにタスクマップ情報を渡しません。回避策として、YFWプロセスは認証のためにAAAを呼び出しますが、AAA認証EXECを使用してこれを行うように指示する必要があります。AAA許可EXECが設定されていない場合、gRPCセッションの許可はスキップされます。

シスコでは、将来的に新しいサービスレベルおよびパスレベルの認証メカニズムを使用してこの問題に対処する予定です。

次の表は、gRPCを使用したタスクベースの許可の適用をまとめたものです。

Cisco IOS XR ソフトウェア	タスクベースの承認は適用されますか。		
	AAAなし	AAAログイン認証を使用するが、AAA認	AAA認可EXECを使

Cisco IOS XR ソフトウェア	タスクベースの承認は適用されますか。		
		可EXECを使用しない場合	用する場合
IOS XR（32ビット）	非サポート	非サポート	非サポート
IOS XR（64ビット）	強制されません。	強制されません。	強制：
IOS XR7(LNT)	強制されません。	強制されません。	強制：

注： gRPCは名前付きメソッドリストをサポートします。デバイスがデフォルト以外の認可方法名を使用している場合は、grpc aaa authorization execとaaa authorization execが一致していることを確認します。

回避策

この脆弱性に対処する回避策はありません。

デバイス設定を確認し、NETCONFまたはgRPCが使用されている場合は、AAA認可EXEC（またはNETCONFの場合はNACM）が有効になっていることを確認します。

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。

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問題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

この問題は、シスコ内部でのセキュリティテストで発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-info-GXp7nVcP

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	2023-9-13

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。