Cisco IOS XRソフトウェアのSNMP管理プレーン保護におけるACLバイパスの脆弱性

アドバイザリーID : cisco-sa-snmp-uhv6ZDeF
初公開日 : 2024-03-13 16:00
バージョン 1.0 : Final
CVSSスコア : 4.3
回避策 : Yes
Cisco バグ ID : CSCwh31469

CVE-2024-20319

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ソフトウェアのUDP転送コードにおける脆弱性により、認証されていない隣接する攻撃者が、設定された管理プレーン保護ポリシーをバイパスし、該当デバイスのSimple Network Management Plane(SNMP)サーバにアクセスする可能性があります。

この脆弱性は、管理プレーン保護を備えたSNMPを使用している場合に、誤ったUDP転送プログラムが原因で発生します。攻撃者は、SNMPサーバが設定された該当デバイスで処理できる宛先アドレスとしてブロードキャストを使用してSNMP操作を実行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、攻撃者は設定されたSNMPポート上のデバイスと通信できる可能性があります。認証されていない攻撃者が設定されたSNMPポートにUDPデータグラムを送信する可能性がありますが、認証されたユーザだけがSNMP要求を使用してデータを取得または変更できます。

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-snmp-uhv6ZDeF

このアドバイザリは、2024年3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。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 XR 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、この脆弱性は、Cisco IOS XR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て、SNMPサーバを有効にして管理プレーン保護を設定しているシスコデバイスに影響を与えていました。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

管理プレーン保護が設定されているかどうかを確認します

管理プレーン保護が設定されているかどうかを確認するには、show running-config control-plane management-planeコマンドを入力します。コマンドの出力が返された場合は、次の例に示すように、管理プレーン保護が設定されています。

<#root>

```
Router#

show running-config control-plane management-plane


!
control-plane
 management-plane
  inband
   interface all
    allow SSH
   !
  !
 !
!
Router#
```

SNMPサーバが設定されているかどうかを確認する

SNMPサーバが設定されているかどうかを確認するには、show running-config snmpコマンドを入力します。デバイスはSNMPv2cまたはSNMPv3で設定できます。コマンドの出力が表示された場合は、次の例に示すようにSNMPサーバが設定されています。

<#root>

```
Router#

show running-config snmp-server
```

```
!
snmp-server community example RO
!
Router#
```

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

この脆弱性の不正利用により、攻撃者は該当デバイスに適用されているアクセスコントロールリスト(ACL)によって提供される保護をバイパスできる可能性があります。この脆弱性の全体的な影響は組織によって異なります。これは、ACLで保護する必要のある資産の重要性によって異なるためです。お客様は、この脆弱性の不正利用がネットワークに与える影響を評価し、独自の脆弱性処理および修復プロセスに従って処理を進める必要があります。

回避策

この脆弱性に対処する回避策はありません。

UDP転送を無効にする

UDP転送は、DNS、TFTP、TACACS、IEN 116 Name Service、NetBIOS Name Service(NBNS)、およびNetBIOS Datagram Service(NBDS)プロトコルに対してデフォルトで有効になっています。UDP転送は、他のUDPプロトコルに対してはデフォルトで有効になっていません。

UDP転送が必要ない場合の回避策は、次の例に示すように、forward-protocol udp disable コマンドを使用して、UDP転送をグローバルに無効にすることです。

<#root>

```
RP/0/RSP0/CPU0:ios#configure terminal
RP/0/RSP0/CPU0:ios(config)#

forward-protocol udp disable
```

```
RP/0/RSP0/CPU0:ios(config)#commit
```

注：UDPブロードキャスト転送がデフォルトのプロトコルに必要な場合、またはUDPブロードキャスト転送がforward-protocol udp <port number>コマンドで設定されている場合、この回避策は使用できません。

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。

修正済みリリース

発行時点では、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左の列はシスコソフトウェアリリースを示し、右の列はリリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースを示しています。

Cisco IOS XR ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
7.11 以前	修正済みリリースに移行。
24.1	24.1.1

Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

シスコはこの脆弱性に対処するSMUをリリースしていません。

不正利用事例と公式発表

Cisco PSIRT では、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は確認しておりません。

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-snmp-uhv6ZDeF

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13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。