Cisco IOS XRソフトウェア専用XMLエージェントのTCPにおけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-iosxr-xml-tcpdos-ZEXvrU2S
初公開日 : 2024-09-11 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 : CSCwj39201

CVE-2024-20390

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ソフトウェアの専用XMLエージェント(DEDICATED XML AGENT)機能の脆弱性により、認証されていないリモートの攻撃者がXML TCPリスニングポート38751でサービス妨害(DoS)を引き起こす可能性があります。

この脆弱性は、入力XMLパケットのエラー検証が適切に行われないことに起因します。攻撃者は、持続的で巧妙に細工されたXMLトラフィックストリームをターゲットデバイスに送信することにより、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、攻撃トラフィックが継続している間にXML TCPポート38751を到達不能に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-iosxr-xml-tcpdos-ZEXvrU2S

このアドバイザリは、2024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。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 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

この脆弱性は、発行時点でDedicated XML Agentが有効になっているCisco IOS XRソフトウェアに影響を与えました。

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。

専用XMLエージェントが設定されているかどうかを確認する

デバイスで専用XMLエージェントが設定されているかどうかを確認するには、show running-config "| include xml"コマンドを使用します。コマンドがxml agent,[1]を返す場合、次の例に示すように、デバイスは脆弱であると見なされます。

<#root>

```
Router#

show running-config | xml
xml agent
```

1. xml agent tty設定コマンドは別のサービスであり、デバイスが影響を受けていることを示すものではありません。実行コンフィギュレーションにxml agent ttyコンフィギュレーションコマンドだけが含まれている場合、そのデバイスは影響を受けません。該当するデバイスは、xml agentコマンドのみを返します。

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 ソフトウェア
- IOS XE ソフトウェア
- 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。ただし、専用XMLエージェント機能が不要で、設定で無効になっている場合、そのデバイスは影響を受けません。

この緩和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

次の表では、左の列にシスコソフトウェアリリースまたはトレインを示します。右の列は、リリース（トレイン）がこのアドバイザリに記載された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最初の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	24.1.2

このドキュメントの発行時点で、シスコはこの脆弱性に対処するために次のSMUをリリースしました。SMUの可用性を含む最新の情報を含む最も完全な情報については、このアドバイザリの上部にあるバグIDの詳細情報のセクションを参照してください。一覧に記載されていないプラットフォームやリリース向けの SMU を必要とするお客様は、サポート部門にご連絡ください。

Cisco IOS XR ソフトウェア リリース	Platform	SMU 名
7.11.2	IOSXRWBD NCS5500	iosxrwbd-7.11.2.CSCwj39201 ncs5500-7.11.2.CSCwj39201

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。

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-iosxr-xml-tcpdos-ZEXvrU2S

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11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。