Cisco IOS XRソフトウェアの接続障害管理におけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-ios-xr-cfm-3pWN8MKt
初公開日 : 2023-09-13 16:00
バージョン 1.0 : Final
CVSSスコア : 4.3
回避策 : No workarounds available
Cisco バグ ID : CSCwd75868

CVE-2023-20233

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Connectivity Fault Management(CFM)機能の脆弱性により、認証されていないリモート攻撃者が該当デバイスにサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、無効な連続性チェックメッセージ(CCM)の不適切な処理に起因します。攻撃者は、巧妙に細工されたCCMを該当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、該当デバイスのピアMEPのメンテナンスエンドポイント(MEP)に関する情報が表示されたときに、CFMサービスがクラッシュ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。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-ios-xr-cfm-3pWN8MKt

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。

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、CFM機能が有効になっているシスコ製品に影響を与えました。Cisco IOS XRソフトウェアでは、CFMはデフォルトで有効になっていません。

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。

デバイス設定の確認

CFMの脆弱性を不正利用するには、ethernet cfmコマンドをグローバルに設定し、デバイスのインターフェイスにmepコマンドを設定する必要があります。

CFMサービスが有効になっているかどうかを確認するには、デバイスにログインして、CLIでshow running-config ethernet cfmコマンドを実行します。グローバルコンフィギュレーションにethernet cfmコマンドがある場合、CFMサービスはデバイスで有効になっています。

次に、CFMサービスが有効になっているデバイスでのshow running-config ethernet cfmコマンドの出力例を示します。

```
<#root>

RP/0/RSP0/CPU0:ios#

show running-config ethernet cfm



ethernet cfm
 domain TestDomain level 7 id string TestDomain
  service TestService down-meps
  continuity-check interval 1s
  mep crosscheck
   mep-id 702 mac-address 1070.fdf8.5555
```

デバイスのいずれかのインターフェイスでmepコマンドが設定されているかどうかを確認するには、show running-config | begin mep domainコマンドを使用します。以下に、show running-config | begin mep domainコマンド：インターフェイスにmepコマンドが設定されているデバイスで使用。

```
<#root>

RP/0/RSP0/CPU0:ios#

show running-config | begin mep domain
```

```
mep domain TestDomain service TestService mep-id 701
```

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

エクスプロイトに成功すると、攻撃者はユーザが情報を表示したときにCFMサービスをクラッシュさせることができます。このクラッシュにより、CFMサービスが再起動します。CFMサービスが複数回クラッシュすると、再起動が最大5分遅れる可能性があります。サービスがダウンしている間は、一部のCFMパケットが失われる可能性があります。

回避策

この脆弱性に対処する回避策はありません。

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）
7.4 以前	修正済みリリースに移行。
7.5	7.5.4
7.6	7.6.3
7.7	7.7.21
7.8	7.8.2
7.9	7.9.1

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。

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、シスコのLogan Sanderson氏による社内セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xr-cfm-3pWN8MKt

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。