Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの Extensible Messaging Client Protocol におけるサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-ios-xmcp-thbAr34t
初公開日 : 2026-08-05 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCwu20827

CVE-2026-20301

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ソフトウェアおよびCisco IOS XEソフトウェアのExtensible Messaging Client Protocol(XMCP)（外部クライアントプロトコルとも呼ばれる）の脆弱性により、認証されていないリモートの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、不正なXMCPパケットの不適切な処理に起因します。攻撃者は、不正な形式のXMCPパケットを該当デバイスに送信することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は該当デバイスのリロードを突発的に引き起こし、その結果DoS 状態が発生する可能性があります。攻撃者がこの脆弱性を不正利用するのに、XMCPクライアントのユーザ名は必要ありません。

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。この脆弱性に対処する緩和策があります。

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-ios-xmcp-thbAr34t

該当製品

脆弱性のある製品

この脆弱性は、Cisco IOSソフトウェアまたはIOS XEソフトウェアの脆弱性が存在するリリースを実行し、XMCPサーバ機能が有効になっているシスコデバイスに影響を与えます。

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。

XMCPサーバー構成の確認

XMCPサーバ機能がデバイスで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、CLIでshow running-config | include service-routing xmcp listenコマンドを使用します。service-routing xmcp listenコマンドが出力に存在する場合、そのデバイスに対してXMCPサーバ機能が有効になっています。

次に、XMCPサーバ機能が有効になっているデバイスでのshow running-config | include service-routing xmcp listenコマンドの出力例を示します。

```
<#root>

Router#

show running-config | include service-routing xmcp listen


service-routing xmcp listen
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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

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 XR 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、緩和策として、管理者は、指定されたアクセスリストに一致するクライアントのみが接続を許可されるように、アクセス制御許可リストを設定することができます。その他のクライアントはすべて拒否されます。次の設定例では、ホスト 192.168.1.1 のみが接続を許可されます。

```
service-routing xmcp listen
 allow-list ipv4 XMCPClientListIPv4
 client username test_xmcp password <removed>
!
ip access-list extended XMCPClientListIPv4
 permit tcp host 192.168.1.1 any
```

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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS 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（例：15.9(3)M2、17.3.3）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 | Check

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

この脆弱性は、内部のセキュリティテストによって発見され、さらに NoisyFood によってシスコに報告されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xmcp-thbAr34t

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	2026 年 8 月 5 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。