Cisco IOS XE ソフトウェアのブロック拡張可能交換プロトコル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-iosxe-bing-MGHrFAkd
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 : CSCwu46548

CVE-2026-20263

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 XEソフトウェアのBlocks Extensible Exchange Protocol(BEEP)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、特定のBEEP SOAP要求を解析する際の不適切な処理に起因します。攻撃者は、該当デバイスに特定のビープ音SOAP要求を送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はデバイスの予期しないリロードを引き起こすことが可能になり、結果として DoS 状態が発生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。これら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-iosxe-bing-MGHrFAkd

該当製品

脆弱性のある製品

ビープ音機能が設定されている場合、この脆弱性はCisco IOS XEソフトウェアに影響を与えます。

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。

デバイス設定の確認

次のいずれかのシナリオで出力が返された場合、デバイスはこの脆弱性の影響を受けます。

NETCONF over BEEPが設定されているかどうかの確認

NETCONF Access for Configurations over BEEP機能を使用すると、NETCONFセッション中にトランスポートプロトコルとしてBEEPを有効にすることができます。Simple Authentication and Security Layer(SASL)を使用してNETCONF over BEEPを有効にするには、まずSASLプロファイルを設定して、デバイスへのアクセスを許可するユーザを指定します。

デバイスでビープ音が設定されているかどうかを確認するには、show running-config | include beep listener CLIコマンドを使用します。次の例に示すように、デバイスが出力を返す場合、そのデバイスはこの脆弱性の影響を受けると見なされます。

```
<#root>

Router#

show running-config | include beep listener


 netconf beep listener 26 acl 101 sasl profile1 encrypt 25
Router#
```

このコマンドで空の出力が返された場合、デバイスにはNETCONF over BEEPが設定されていません。

BEEPリスナーが構成されているかどうかを確認します

Cisco IOS XEソフトウェアでは、特権レベル15のユーザがbingd device <port> CLIコマンドを使用してビープ音のリスナーを作成できます。特定のデバイスでビープ音が有効になっているかどうかを確認するには、次の例に示すようにshow processes | include bingd CLIコマンドの出力を調べます。

```
<#root>

Router#

show processes | include bingd


 330 Mwe 578A2325470C             0          1       0   9776/12000  0 bingd_raw_proc
Router#
```

このコマンドで空の出力が返された場合、デバイスにはビープ音リスナーが設定されていません。

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 ソフトウェア
- 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。

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

この脆弱性を報告していただいた Guan Yi 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-bing-MGHrFAkd

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。