Cisco IOS、IOS XE、およびIOS XRソフトウェアのTWAMP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-twamp-kV4FHugn
初公開日 : 2025-05-07 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 : CSCve33776 CSCwk80897 CSCwm63229

CVE-2025-20154

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Two-Way Active Measurement Protocol(TWAMP)サーバ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のリロードを引き起こし、その結果、サービス妨害(DoS)状態が発生する可能性があります。Cisco IOS XRソフトウェアでは、デバッグが有効になっていると、この脆弱性によりipsla_ippm_serverプロセスの予期しないリロードが発生する可能性があります。

この脆弱性は、特別に巧妙に細工されたTWAMP制御パケットを処理する際の範囲外のアレイアクセスに起因します。攻撃者は、巧妙に細工されたTWAMP制御パケット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。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。

注：Cisco IOS XRソフトウェアでは、ipsla_ippm_serverプロセスだけが、デバッグが有効な場合にのみ予期せずにリロードされます。Cisco IOS XRソフトウェアの脆弱性の詳細は次のとおりです。

セキュリティ影響評価(SIR)：低
CVSS ベーススコア：3.7
CVSSベクトル：CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L

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-twamp-kV4FHugn

このアドバイザリは、2025年5月に公開されたCisco IOSソフトウェアおよびIOS XEソフトウェアの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リンクの一覧については、『シスコイベントレスポンス：Cisco IOSおよびIOS XEソフトウェアに関するセキュリティアドバイザリ公開資料（半年刊、2025年5月）』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、TWAMPサーバ機能が有効になっている次のシスコ製品に影響を与えます。

- デバッグを有効にした場合としなかった場合のIOSソフトウェアへの影響
- IOS XE ソフトウェア
  - リリース16.6.1 ~ 17.2.3が影響を受けるのは、デバッグコマンドdebug ip sla trace twamp connectionがアクティブな場合だけです。
  - その他すべてのリリース（最初の修正済みリリースまで）で、この脆弱性の影響を受けるためにはデバッグを有効にする必要はありません。
- IOS XRソフトウェアは、デバッグコマンドdebug ipsla trace twamp connectionがアクティブな場合にのみ影響を受けます。

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。

TWAMPサーバ設定の確認

Cisco IOSおよびCisco IOS XEソフトウェア

TWAMPサーバ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、show running-config | include ip sla server twamp CLIコマンドを使用します。TWAMPサーバ機能が有効になっているデバイスは、この脆弱性の影響を受けます。

次の例は、TWAMPサーバが有効になっているデバイスの出力を示しています。

<#root>

```
Router#
show running-config | include ip sla server twamp


ip sla server twamp
```

```
Router#
```

このコマンドで出力が返されない場合、またはエラーが返される場合、デバイスは影響を受けません。

Cisco IOS XEソフトウェアを実行しているデバイスでTWAMPデバッグが有効になっているかどうかを確認するには、show debug | include TWAMP Server Connection TRACE CLIコマンドを使用します。

次の例は、IP SLAデバッグが有効になっているデバイスの出力を示しています。

```
<#root>

Router#

show debug | include TWAMP Server Connection TRACE


IPPM TWAMP Server Connection TRACE debug all

Router#
```

コマンドから出力が返されない場合、またはエラーが返される場合、デバイスのデバッグは有効になっていません。

Cisco IOS XR ソフトウェア

TWAMPサーバ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、show running-config ipsla server twamp CLIコマンドを使用します。TWAMPサーバ機能が有効になっているデバイスは、この脆弱性の影響を受けます。

次に、IP SLA レスポンダが有効になっているデバイスの出力例を示します。

```
<#root>

RP/0/RP0/CPU0:IOSXR#

show running-config ipsla server twamp

 ipsla

server twamp

 !
```

```
RP/0/RP0/CPU0:IOSXR#
```

このコマンドで出力が返されない場合、またはエラーが返される場合、デバイスは影響を受けません。

TWAMPデバッグ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、show debug | include ipsla trace twamp connection CLIコマンドを使用します。TWAMPサーバ機能が設定されており、デバイスでデバッグが有効になっている場合、そのデバイスはこの脆弱性の影響を受けます。

次の例は、IP SLAデバッグが有効になっているデバイスの出力を示しています。

```
<#root>

RP/0/RP0/CPU0:IOSXR#

show debug | include ipsla trace twamp connection


Wed Mar 26 16:00:00.000 UTC

ipsla trace twamp connection

 flag is ON with value 0
RP/0/RP0/CPU0:IOSXR#
```

コマンドから出力が返されない場合、またはエラーが返される場合、デバイスのデバッグは有効になっていません。

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。

- Meraki 製品
- 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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリ

リースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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完全なアップグレード ソリューション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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

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記載しています。右側の列は、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）
24.2 以前	修正済みリリースに移行。
24.3	24.3.2
24.4.1 以降	影響なし。

注：必要な修正の性質上、シスコはこの脆弱性に対処するSMUを開発できません。ソフトウェアのアップグレードが必要です。

シスコの 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済みリリース情報のみを検証します。

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 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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-twamp-kV4FHugn

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	2025年5月7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。