Catalyst 9000シリーズスイッチ用Cisco IOS XEソフトウェアのサービス妨害(DoS)の脆弱性

High

アドバイザリーID : cisco-sa-cat9k-PtmD7bgy
初公開日 : 2025-09-24 16:00
バージョン 1.0 : Final
CVSSスコア : 7.4
回避策 : No workarounds available
Cisco バグ ID : CSCwn45401

CVE-2025-20311

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

Catalyst 9000シリーズスイッチ用Cisco IOS XEソフトウェアの特定のイーサネットフレームの処理における脆弱性により、認証されていない隣接する攻撃者が出力ポートをブロックさせ、すべての発信トラフィックをドロップする可能性があります。

この脆弱性は、巧妙に細工されたイーサネットフレームの不適切な処理に起因します。攻撃者は、該当スイッチを介して巧妙に細工されたイーサネットフレームを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、巧妙に細工されたフレームの転送先である出力ポートですべてのフレームの廃棄を開始させ、その結果サービス拒否(DoS)状態を引き起こす可能性があります。

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-cat9k-PtmD7bgy

このアドバイザリは、Cisco IOS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公開の2025年9月リリースの一部です。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9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、Cisco 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、トランクポート、Cisco TrustSec対応ポート、またはMACSec対応ポートが有効になっている次のCisco Catalyst 9000スイッチングファミリプラットフォームに影響を与えます。

- Catalyst 9200 シリーズ スイッチ
- Catalyst 9300 シリーズ スイッチ
- Catalyst 9400 シリーズ スイッチ
- Catalyst 9500 シリーズ スイッチ
- Catalyst 9600 シリーズ スイッチ

Meraki CS 17.2.2より前のソフトウェアを実行しているMeraki MS390およびCisco Catalyst 9300シリーズスイッチが影響を受けます。リリース17.15.4より前のCisco IOS XEソフトウェアリリースを実行しているCatalyst Wireless LAN Controller用のCloud-Managed Hybrid Operating Mode(CMF)も影響を受けます。これは、Cisco IOS XEソフトウェアリリース17.15.4で修正されています。

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

デバイスでトランクポートが有効になっているかどうかの確認

デバイスでトランクポートが有効になっているかどうかを確認するには、Administrator権限を使用してデバイスのCLIに接続し、show running-config | include switchport mode trunk|dynamic|dot1q-tunnelコマンドを使用します。次の例に示すように、出力が返される場合、デバイスは影響を受けます。

<#root>

```
Switch#
show running-config | include switchport mode trunk|dynamic|dot1q-tunnel


 switchport mode trunk
Switch#
```

デバイスにCisco TrustSec対応ポートがあるかどうかを確認する

デバイスでCisco TrustSec対応ポートが使用されているかどうかを確認するには、Administrator 権限を使用してデバイスのCLIに接続し、show running-config | include cts manual コマンドを使用します。次の例に示すように、出力が返される場合、デバイスは影響

を受けます。

```
<#root>

Switch#

show running-config | include cts manual
 cts manual


Switch#
```

デバイスにMACsec対応ポートがあるかどうかを確認する

デバイスでMACsecが有効になっているポートがあるかどうかを確認するには、Administrator権限を使用してデバイスのCLIに接続し、show macsec summaryコマンドを使用します。返された出力にインターフェイスが含まれている場合、デバイスは次の例のように影響を受けます。

```
<#root>

Switch#

show macsec summary


Interface                     Transmit SC          Receive SC
Gi1/0/1                             0                    0
Switch#
```

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。

- Catalyst 9800 シリーズ ワイヤレス コントローラ
- IE9300高耐久性シリーズスイッチ
- IOS ソフトウェア
- IOS XR ソフトウェア
- NX-OS ソフトウェア

詳細

特定の巧妙に細工されたイーサネットフレームの処理により、該当ポートの出力ポートFIFOキューがスタックし、その結果、ポートがすべての発信トラフィックをドロップする可能性があります。次に例を示します。

```
<#root>

Switch#show interfaces tenGigabitEthernet 6/0/1 | include Total output drops
 Input queue: 0/375/0/0 (size/max/drops/flushes);

Total output drops: 461992

Switch#
```

このコマンドを複数回繰り返すと、Total output dropsの値が継続的に増加します。これは、トラフィックがインターフェイスを経由して転送されていないことを示します。

この状態から回復するには、まず、巧妙に細工されたフレームの送信元を特定します。次に、そのデバイスを削除するか、VLANまたはMAC ACLを使用してそのデバイスをブロックします。細工されたフレームの送信元が削除されたら、デバイスをリロードします。これは、デバイスを回復する唯一の方法です。

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

シスコでは、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、回避策や緩和策は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復し、本アドバイザリで説明されている障害の発生を回避するために、お客様には本アドバイザリで説明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、Cisco Technical Assistance Center(TAC)の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-cat9k-PtmD7bgy

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9月24日

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。