Catalyst 9000シリーズスイッチ用Cisco IOS XEソフトウェアのDHCPスヌーピングにおけるDoS脆弱性

アドバイザリーID : cisco-sa-bootp-WuBhNBxA
初公開日 : 2026-03-25 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : Yes
Cisco バグ ID : CSCwq07617

CVE-2026-20084

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DHCPスヌーピング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VLAN間でBOOTPパケットを転送させ、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。

この脆弱性は、Cisco Catalyst 9000シリーズスイッチでのBOOTPパケットの不適切な処理に起因します。攻撃者は、該当デバイスにBOOTP要求パケット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、攻撃者がBOOTPパケットをVLAN間で転送できるようになり、BOOTP VLANのリークが発生してCPU使用率が高くなる可能性があります。これにより、デバイスが（コンソールまたはリモート管理を通じて）到達不能になり、トラフィックを転送できなくなり、DoS状態が発生します。

注：この脆弱性は、ユニキャストまたはブロードキャストのBOOTPパケットによって不正利用され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。本脆弱性に対処する回避策がいくつかあります。

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-bootp-WuBhNBxA

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2026年3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、『

Cisco Event Response: March 2026 Semiannual Cisco IOS and IOS XE 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

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、次の設定条件を持つCisco Catalyst 9000シリーズスイッチに影響を与えます。

- IP DHCPスヌーピングが有効である
- ip helper-addressは、スイッチ仮想インターフェイス(SVI)で設定されます
- ip helper-address のネクストホップはサブインターフェイスです
- サブインターフェイスの1つにネイティブ VLANが設定されています

これら4つの条件が当てはまる場合、BOOTPパケットは送信元インターフェイスから、ネイティブVLANが設定されているサブインターフェイスに転送されます。また、ネイティブVLANがIP DHCPスヌーピング範囲の一部である場合、CPU使用率が増加し、DoS状態が発生します。

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

デバイスに脆弱性のある設定があるかどうかを確認するには、次の方法を使用します。

デバイスでIP DHCPスヌーピングが有効になっているかどうかの確認

特定のデバイスでIP DHCPスヌーピング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 ip dhcp snooping execコマンドを使用します。出力が返された場合、デバイスではIP DHCPスヌーピングが有効になっています。次の例は、VLAN 16、32、および64でIP DHCPスヌーピングが有効になっているデバイスを示しています。

```
<#root>

Router#

show running-config | include ip dhcp snooping


ip dhcp snooping vlan 16, 32, 64


ip dhcp snooping
```

```
Router#
```

出力が返されない場合、デバイスは影響を受けません。

デバイスのSVIでip helper-addressが設定されているかどうかを確認する

デバイスのSVI上でip helper-addressが設定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 | section interface Vlan execコマンドを使用します。返された出力に、ip helper-address <ip_address>で始まる行が含まれている場合、そのSVIの下にIPヘルパーアドレスが設定されています。次の例は、SVI Vlan64でIPヘルパーアドレスが設定されているデバイスを示しています。

<#root>

```
Router#
show running-config | section interface Vlan


!
interface Vlan16
 ip address 10.101.16.1 255.255.255.0
 no ip redirects
 ip ospf 1 area 0
!
interface Vlan32
 ip address 10.101.32.1 255.255.255.0
 ip ospf 2 area 0
!
interface Vlan64
 ip address 10.101.64.1 255.255.255.0
 ip helper-address 10.100.128.1


 no ip redirects
 ip ospf 3 area 0
!
Router#
```

出力が返されない場合、または出力にip helper-addressコマンドが含まれていない場合、そのデバイスは影響を受けません。

いずれかのサブインターフェイスでネイティブVLANが設定されているかどうかを確認する

デバイスのサブインターフェイスにネイティブVLANが設定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 | section ^interface execコマンドを使用します。サブインターフェイスの下に出力にencapsulation dot1q <value> native が含まれている場合、ネイティブVLANはサブインターフェイスで設定さ

れます。次の例は、サブインターフェイスtwentyFiveGigE 1/0/2.2にネイティブVLANが設定されているデバイスを示しています。

```
<#root>

Router#

show running-config | section ^interface


!
interface twentyFiveGigE 1/0/2
 no switchport
 no ip address
 ip ospf network point-to-point
 ip ospf 4 area 0
!
interface twentyFiveGigE 1/0/2.1
 encapsulation dot1Q 16
 ip address 10.100.16.1 255.255.255.252
 no ip redirects
 ip ospf network point-to-point
 ip ospf 4 area 0
!
interface twentyFiveGigE 1/0/2.2
 encapsulation dot1Q

32 native


 ip address 10.100.32.1 255.255.255.252
 no ip redirects
 ip ospf network point-to-point
 ip ospf 5 area 0
!
Router#
```

出力のencapsulation dot1Q <value>パラメータにnativeパラメータが含まれていない場合、そのデバイスは影響を受けません。

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。

BOOTPトラフィックを処理する必要のない環境では、該当するデバイスでip dhcp relay bootp ignoreを設定します。

この回避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 Cisco Cisco Technical Assistance Center（TAC）サポートケースの解決中に発見されました。

シスコは、この脆弱性のトラブルシューティングと報告を支援してくださったMatthijs van der Wal氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bootp-WuBhNBxA

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3月25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。