# Cisco IOS XEソフトウェアのDHCPスヌーピングにおけるDenial of Service(DoS)の脆弱性

High

アドバイザリーID : cisco-sa-iosxe-dhcpsn-dos-xBn8Mtks
CVE-2025-20162
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 : Yes
Cisco バグ ID : CSCwm45385

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スヌーピングセキュリティ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インターフェイスキューウェッジ全体を発生させ、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、DHCP要求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DHCP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、パケットがキュー内でウェッジ状態になり、該当システムのダウンストリームデバイスでDoS状態が発生し、キューをドレインするためにシステムを再起動する必要が生じる可能性があります。

注：この脆弱性は、DHCPスヌーピングが有効になっていないVLAN上のユニキャストまたはブロードキャストDHCPパケットのいずれかで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-iosxe-dhcpsn-dos-xBn8Mtks

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、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、デバイスに設定されている少なくとも1つのVLANに対してDHCPスヌーピングが有効になっている次のシスコ製品に影響を与えます（すべてではありません）。

- 1100シリーズサービス統合型ルータ(ISR)
- Catalyst 8200 シリーズ エッジ プラットフォーム
- Catalyst 8300 シリーズ エッジ プラットフォーム

注：DHCPスヌーピングが有効になっているVLANでパケットが受信された場合、そのパケットは保持されません。DHCPスヌーピングが有効になっていないVLANでパケットが受信された場合、そのパケットは保持されます。

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

DHCPスヌーピングが、デバイス上のすべてではなく、一部のVLANに対して有効になっているかどうかを確認するには、次の例で示すように、show ip dhcp snoopingコマンドを実行します。

```
<#root>

Router#

show ip dhcp snooping


Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled

DHCP snooping is configured on following VLANs:
2
DHCP snooping is operational on following VLANs:
2

Proxy bridge is configured on following VLANs:
none
Proxy bridge is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 4c77.6d2e.3bf1 (MAC)

Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
```

```
Verification of giaddr field is enabled

DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
Router#
```

アクティブなVLANをすべて表示するには、次の例で示すようにshow vlanコマンドを使用します。

```
<#root>

Router#

show vlan


VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default

active

Gi0/1/0, Gi0/1/1, Gi0/1/2
                                                Gi0/1/3
2    VLAN0002

active


1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

## 脆弱性を含んでいないことが確認された製品

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
- ISR 1000シリーズルータ
- Meraki 製品
- NX-OS ソフトウェア

# 詳細

一時的な対策を使用して、デバイスをリロードできるまでトラフィックを通過させる

この脆弱性がエクスプロイトされ、攻撃が停止した場合、管理者は、影響を受けるインターフェイスに現在設定されている値よりも大きい最大hold-queue値を設定して、デバイスがリロード可能になるまでトラフィックを通過させることができます。次の例は、hold-queue inインターフェイス設定コマンドを使用して、値を350に設定する方法を示しています。

<#root>

```
Router#
configure terminal
Router(config)#
interface
 gigabitEthernet 1
Router(config-if)#
hold-queue 350 in
```

Cisco IOS Embedded Event Managerによるキューウェッジの監視と検出

この脆弱性によって引き起こされるインターフェイスキューのウェッジを監視および検出するために、管理者はTool Command Language(Tcl)に基づくCisco IOS Embedded Event Manager(EEM)ポリシーを使用できます。 このポリシーにより、管理者はCisco IOS XEソフトウェアを実行しているデバイスのインターフェイスをモニタし、入力キューがいっぱいになったことを検出できます。Cisco IOS EEMがこの脆弱性のエクスプロイトの可能性を検出すると、ポリシーからネットワーク管理者にアラートが送信されます。ネットワーク管理者は、入力キューをクリアするために、デバイスのアップグレード、適切な移行、またはリロードを実行することを決定できます。

TCLスクリプトは、Interface Input Queue Monitorでダウンロードできます。

# セキュリティ侵害の痕跡

該当するインターフェイスを特定するには、次のコマンドを実行します。

<#root>

```
Router#
show interfaces | include line|Input

GigabitEthernet1 is up, line protocol is up
  Input queue:
```

**376**

/

**375**

/0/0 (size/

**max**

/drops/flushes); Total output drops: 0

サイズの値がmaxの値よりも大きい場合、入力キューはブロックされます。

## 回避策

この脆弱性に対処する回避策はありません。次の例に示すように、管理者はip dhcp snooping vlan ?コマンドを使用してすべてのVLANでDHCPスヌーピングを有効にできます。

<#root>

Device-1(config)#

**ip dhcp snooping vlan ?**

 WORD DHCP Snooping vlan first number or vlan range, example: 1,3-5,7,9-11

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。

## 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 TAC 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-iosxe-dhcpsn-dos-xBn8Mtks

## 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

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。