複数のシスコ製品スイッチ統合セキュリティ機能のDHCPv6におけるDoS脆弱性

High

アドバイザリーID : cisco-sa-sisf-dos-ZGwt4DdY
初公開日 : 2025-05-07 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 : CSCvq14413 CSCwk02785 CSCwk04230 CSCwj88828 CSCwk02672 CSCvo13585

CVE-2025-20191

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、Cisco IOS XEソフトウェア、Cisco NX-OSソフトウェア、およびCisco Wireless LAN Controller(WLC)AireOSソフトウェアのSwitch Integrated Security Features(SISF)の脆弱性により、認証されていない隣接する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、DHCPv6パケットの不適切な処理に起因します。攻撃者は、巧妙に細工されたDHCPv6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。

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-sisf-dos-ZGwt4DdY

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、次のシスコソフトウェアの脆弱性が存在するリリースを実行し、SISFが有効になっているシスコ製品に影響を与えます。

- IOSソフトウェア(CSCwk04230)
- IOS XEソフトウェア(CSCvq14413)
- WLC用のIOS XEソフトウェア(CSCvo13585)[1]
- WLC AireOSソフトウェア(CSCwj88828)

1. WLC用のCisco IOS XEソフトウェアについては、16.11以前のリリースのみが脆弱であり、サポートは終了しています。詳細については、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。

この脆弱性は、Cisco NX-OSソフトウェアの脆弱性が存在するリリースを実行し、SISFが有効になっている次のシスコ製品にも影響を与えます。

- Nexus 3000シリーズスイッチ(CSCwk02672)
- Nexus 7000シリーズスイッチ(CSCwk02785)
- スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ(CSCwk02672)

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

Cisco IOS および IOS XE ソフトウェア

Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアでは、SISFはデフォルトで有効になっていません。特定のデバイスでSISFが有効になっているかどうかを確認するには、show device-tracking policiesまたはshow ipv6 snooping policies CLIコマンドを使用します（このコマンドはソフトウェアリリースによって異なる場合があります）。 出力に何らかのポリシーが表示されている場合、SISFは有効です。次の例は、該当するデバイスでこれらのコマンドが発行された場合の出力例を示しています。

<#root>

```
switch#

show device-tracking policies

Target               Type  Policy               Feature        Target range
vlan 1150            VLAN  default              Device-tracking vlan all
switch#
```

```
show ipv6 snooping policies

Target              Type  Policy              Feature        Target range
vlan 1150           VLAN  default             Device-tracking vlan all
```

WLC用Cisco IOS XEソフトウェア

WLC用のCisco IOS XEソフトウェアでは、SISFはデフォルトで有効になっています。デバイスでSISFが有効になっているかどうかを確認するには、show wireless device-tracking database ip CLIコマンドを使用します。出力に何らかのエントリが表示されている場合は、次の例に示すように、SISFが有効になります。

```
<#root>

wlc#

show wireless device-tracking database ip

IP              ZONE/VRF-TABLE-ID    STATE        DISCOVERY     MAC          VRF-NAME
-------------------------------------------------------------------------------------
fd12:3456:789a:1::1 0x00000000       Reachable    IPv6 NDP      aaaa.aaaa.aaaa
10.10.10.20         0x00000000       Reachable    IPv4 DHCP     bbbb.bbbb.bbbb
```

Cisco WLC AireOSソフトウェア

Cisco WLC AireOSソフトウェアでは、この脆弱性の影響を受けるデバイスはIPv6の設定によって異なります。デバイスが影響を受けるかどうかを確認するには、show ipv6 summary CLIコマンドを使用します。次の例に示すように、出力で「Global Config」が「enabled」とマーキングされている場合、そのデバイスはこの脆弱性の影響を受けます。

```
<#root>

(controller)>

show ipv6 summary
Global Config

.............................

Enabled


.
.
.
```

Cisco NX-OS ソフトウェア

Cisco NX-OSソフトウェアでは、SISFはデフォルトで有効になっていません。デバイスでSISFが有効になっているかどうかを確認するには、show ipv6 snooping policies CLIコマンドを使用します。出力に何らかのポリシーが表示されている場合、SISFは有効です。次に、該当するデバイスでこれらのコマンドが発行された場合の出力例を示します。

<#root>

switch#

show ipv6 snooping policies

```
Target              Type  Policy               Feature        Target range
vlan 100            VLAN  dhcpguard-sample-policy DHCP Guard     vlan all
vlan 200            VLAN  dhcpguard-sample-policy-2 DHCP Guard     vlan all
vlan 300            VLAN  default              Snooping       vlan all
```

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。

- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Firepower 4100 シリーズ
- Firepower 9300 セキュリティ アプライアンス
- IOS XR ソフトウェア
- MDS 9000 シリーズ マルチレイヤ スイッチ
- Meraki 製品
- VMware vSphere 向け Nexus 1000 Virtual Edge
- Nexus 5500 プラットフォーム スイッチ
- Nexus 5600 プラットフォーム スイッチ
- Nexus 6000 シリーズ スイッチ
- ACI モードの Nexus 9000 シリーズ ファブリック スイッチ
- Cisco Secure Firewall 3100 シリーズ
- Cisco Secure Firewall 4200 シリーズ
- UCS 6300 シリーズ ファブリック インターコネクト
- UCS 6400 シリーズ ファブリック インターコネクト
- UCS 6500 シリーズ ファブリック インターコネクト

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のリリースを記載しています。右側の列は、リリース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。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

ワイヤレスLANコントローラ用Cisco IOS XE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）
16.11以前[1]	修正済みリリースに移行。
16.12	脆弱性なし
17	脆弱性なし

1. WLCリリース16.11以前のCisco IOS XEソフトウェアはサポートが終了しています。この脆弱性の修正を含むサポート対象リリースに移行することをお勧めします。

Cisco WLC AireOS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）
8.9 以前	修正済みリリースに移行。
8.10	8.10.196.0

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

Cisco NX-OS ソフトウェア

お客様が Cisco NX-OS 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。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。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. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。
4. リリース番号を入力します。たとえば、Cisco Nexus 3000 シリーズ スイッチの場合は 7.0(3)I7(5)、ACI モードの Cisco NX-OS ソフトウェアの場合は 14.0(1h) です。
5. [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 | Cisco NX-OS ソフトウェア
あらゆるプラットフォーム

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

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-sisf-dos-ZGwt4DdY

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。