Application-Centric Infrastructure モードの Cisco Nexus 9000 シリーズ ファブリック スイッチにおける DHCP バージョン 6 機能の DoS に対する脆弱性

アドバイザリーID : cisco-20180718-nexus-9000-dos
CVE-2018-0372
初公開日 : 2018-07-18 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 : CSCvg38918

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

Application-Centric Infrastructure（ACI）モードの Cisco Nexus 9000 シリーズ ファブリック スイッチにおける DHCPv6 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デバイスのシステム メモリを枯渇させ、結果として該当システムがサービス妨害（DoS）状態となる可能性があります。

この脆弱性は、該当デバイスのインターフェイスが DHCPv6 パケットを受信したときの不適切なメモリ管理に起因します。攻撃者は、DHCPv6 パケットを処理するように設定された該当デバイスに、巧妙に細工された DHCPv6 パケットを大量に送信することによってこの脆弱性をエクスプロイトする可能性があります。エクスプロイトが成功すると、システム メモリが枯渇し、最終的に該当デバイスのリブートが引き起こされる可能性があります。この脆弱性は IPv6 プロトコル パケットによってのみエクスプロイトが可能です。IPv4 プロトコル パケットではエクスプロイトされません。

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-20180718-nexus-9000-dos

該当製品

脆弱性のある製品

ソフトウェア バージョン 13.0(1k) を稼働させている Cisco Nexus 9000 シリーズ ファブリック スイッチが ACI モードの場合に、この脆弱性の影響を受けます。

この脆弱性は、ブリッジ ドメイン（BD）でユニキャスト ルーティングが有効化されている場合にのみエクスプロイトが可能です。脆弱性のエクスプロイトには、DHCP および DHCP リレーが設定されている必要がありません。

NX-OS ソフトウェア リリースの判別

管理者は、デバイスの CLI で show version コマンドを使用することによって、デバイスで実行されている NX-OS ソフトウェアのバージョンを確認できます。次の例は 11.2(2) リリースを示しています。

```
<#root>

nxos-n9k-aci#

show version

Cisco Nexus Operating System (NX-OS) Software
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
Software
  BIOS:      version N/A
  kickstart: version 11.2(2) [build 11.2(1.184)]
  system:    version

11.2(2)

 [build 11.2(1.184)]
```

APIC ソフトウェア リリースの判別

Cisco Application Policy Infrastructure Controller（APIC）と ACI モードの Cisco Nexus 9000 シリーズ ファブリック スイッチの間では、ソフトウェアは 1 対 1 で対応しています。つまり、Cisco NX-OS ソフトウェア バージョン番号の左端の 1 を削除したものが、使用中の Cisco APIC リリースとなります。前の例では、Cisco APIC ソフトウェアのバージョンは 1.2(2) となります。

ユニキャスト ルーティングが有効化されているか判別する

管理者は、デバイスの CLI で次のコマンドを使用することによって、デバイスでユニキャスト ルーティングが有効化されているかどうかを確認できます。

<#root>

nxos-n9k-aci#

moquery -d uni/tn-ag/BD-bd1 | egrep "unicastRoute"

unicastRoute   : yes

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記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコは、本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 2100 シリーズ
- Firepower 4100 シリーズ次世代ファイアウォール
- Firepower 9300 セキュリティ アプライアンス
- MDS 9000 シリーズ マルチレイヤ ディレクタ スイッチ
- Nexus 1000V シリーズ スイッチ
- Nexus 1100 シリーズ クラウド サービス プラットフォーム
- Nexus 2000 シリーズ スイッチ
- Nexus 3000 シリーズ スイッチ
- Nexus 3500 プラットフォーム スイッチ
- Nexus 3600 プラットフォーム スイッチ
- Nexus 5000 シリーズ スイッチ
- 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 7000 シリーズ スイッチ
- Nexus 7700 シリーズ スイッチ
- NX OS モードの Nexus 9000 シリーズ スイッチ
- Nexus 9500 R シリーズ ラインカードおよびファブリック モジュール
- UCS 6100 シリーズ ファブリック インターコネクト
- UCS 6200 シリーズ ファブリック インターコネクト
- UCS 6300 シリーズ ファブリック インターコネクト

セキュリティ侵害の痕跡

脆弱性が工クスプロイトされると、該当するデバイスのリロードが発生してコア ファイルが生成される場合があります。Cisco Technical Assistance Center（TAC）に連絡して、コア ファイルの確認と、その内容がこの脆弱性に起因するものかどうかを判断してください。

管理者は、リーフ ノード プロンプトから ps aux | grep 'dhcp_snoop\|VSZ'をリーフノードプロン

プトから実行します。デバイスの予期しない再起動を防ぐために、表示される値が 3 GB を超えた場合はデバイスをリブートすることを推奨します。次の例は、仮想メモリ サイズ（VSZ）が 3 GB に達していないデバイスを示しています。

<#root>

nxos-n9k-aci#

ps aux | grep 'dhcp_snoop\|VSZ'

```
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root     13225  0.0  1.5 1712896 382940 ?      Ssl  Jun26   0:26 /isan/bin/dhcp_snoop
admin    21444  0.0  0.0   2272   524 pts/0    SN+  11:35   0:00 grep dhcp_snoop\|VSZ
```

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。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。

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート（Cisco Security Advisories and Alerts）] 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 Cisco Service Contract 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 POS から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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

この脆弱性は、ACI モードの Cisco Nexus 9000 シリーズ ファブリック スイッチ バージョン 13.0(2k) 以降のリリースで修正されています。

該当バージョンのデバイスを実行しているすべてのお客様には、最新のメンテナンス バージョンまたは最新の Long-Lived バージョンにアップグレードすることを推奨します。シスコでは、お客様がhttps://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/recommended-release/b_Recommended_Cisco_ACI_Releases.htmlページにアクセスして、どの修正済みリリースを選択するかを確認することを推奨します。

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-20180718-nexus-9000-dos

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	2018 年 7 月 18 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。