Cisco IOS XRソフトウェアのDHCPバージョン4サーバにおけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-iosxr-dhcp-dos-3tgPKRdm
初公開日 : 2024-03-13 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : No workarounds available
Cisco バグ ID : CSCwf83090

CVE-2024-20266

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 XRソフトウェアのDHCPバージョン4(DHCPv4)サーバ機能における脆弱性により、認証されていないリモートの攻撃者がdhcpdプロセスのクラッシュを引き起こし、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、特定のDHCPv4メッセージが該当デバイスで処理されるときに不適切に検証されることに起因します。攻撃者は、該当デバイスに不正なDHCPv4メッセージを送信することで、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、dhcpdプロセスがクラッシュする可能性があります。dhcpdプロセスが再起動する間（約2分かかります）は、影響を受けるデバイスでDHCPv4サーバサービスが利用できません。これにより、その期間中にネットワークに参加し、影響を受けるデバイスのDHCPv4サーバに依存するクライアントへのネットワークアクセスが一時的に妨げられる可能性があります。

注：

- dhcpdプロセスだけがクラッシュし、最終的には自動的に再起動します。ルータはリロードしません。
- この脆弱性はDHCPv4にのみ適用されます。DHCPバージョン6(DHCPv6)は影響を受けません。

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-sa-iosxr-dhcp-dos-3tgPKRdm

このアドバイザリは、2024年3月に公開されたCisco IOS XRソフトウェアセキュリティアドバイザリバンドルの一部です。アドバイザリとリンクの一覧については、Cisco Event Response: March 2024 Semiannual Cisco IOS XR 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

公開時点で、この脆弱性は、DHCPv4サーバ機能またはDHCPv4プロキシ機能が有効になっているCisco IOS XRソフトウェアに影響を与えました。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

DHCPv4設定の確認

デバイスでDHCPv4サーバ機能またはDHCPv4プロキシ機能が有効になっているかどうかを確認するには、デバイスCLIの特権EXECモードでshow running-config dhcp ipv4コマンドを実行して、少なくとも1つのインターフェイスに直接または間接的に（基本プロファイルを介して）バインドされているサーバプロファイルが存在するかどうかを確認します。

次に、DHCPv4サーバプロファイルTESTがインターフェイスGigabitEthernet0/0/0/0に直接バインドされているデバイスでのshow running-config dhcp ipv4コマンドの出力例を示します。

```
<#root>
dhcp ipv4


profile
 TEST
server


  .
  .
  .
 !

interface
 GigabitEthernet0/0/0/0
server profile
 TEST
```

次の例は、DHCPv4サーバプロファイルDHCP_SERVERとDEFAULT_PROFILEがベースプロファイルDHCP_BASEを介してインターフェイスGigabitEthernet0/0/0/0に間接的にバインドされているデバイスでのshow running-config dhcp ipv4コマンドの出力を示しています。

```
<#root>
dhcp ipv4


profile
 DHCP_BASE
base

  match option 60 41424355
profile
 DHCP_SERVER
server

  default
profile
 DEFAULT_PROFILE
server

  .
  .
  .
 !

profile
 DHCP_SERVER
server

  .
  .
  .
 !

profile
 DEFAULT_PROFILE
server

  .
```

```
  .
  .
 !

interface
 GigabitEthernet0/0/0/0
base profile
 DHCP_BASE
```

次に、DHCPv4プロキシプロファイルPROXYがインターフェイスGigabitEthernet0/0/0/0に直接バインドされているデバイスでのshow running-config dhcp ipv4コマンドの出力例を示します。

```
<#root>
dhcp ipv4



profile
 PROXY
proxy

  helper-address vrf default 192.168.23.7 giaddr 192.168.23.11
 !

interface
 GigabitEthernet0/0/0/0
proxy profile
 PROXY
```

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、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 XE 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。

修正済みソフトウェア

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アップグレード ソリューション一式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。

修正済みリリース

発行時点では、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左側の列にはシスコソフトウェアリリース、右側の列に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リリースが示されています。

Cisco IOS XR 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）
7.9 以前	修正済みリリースに移行。
7.10	修正済みリリースに移行。
7.11	7.11.1
24.1	24.1.1

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されたリリース情報のみを検証します。

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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dhcp-dos-3tgPKRdm

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	2024年3月13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。