# Cisco NX-OSソフトウェアのExternal Border Gateway ProtocolにおけるDoS脆弱性


アドバイザリーID : cisco-sa-nxos-ebgp-dos-L3QCwVJ
初公開日 : 2024-02-28 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 : CSCwh96478 CSCwh09703

CVE-2024-20321

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 NX-OSソフトウェアのExternal Border Gateway Protocol(eBGP)実装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、eBGPトラフィックが共有のハードウェアレートリミッタキューにマッピングされることに起因します。攻撃者は、特定の特性を持つ大量のネットワークトラフィックを該当デバイスを介して送信することで、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、攻撃者はeBGPネイバーセッションをドロップさせ、ネットワークでDoS状態を引き起こす可能性があります。

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-nxos-ebgp-dos-L3QCwVJ

このアドバイザリは、2024年2月に公開されたCisco FXOSおよびNX-OS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: February 2024 Semiannual Cisco FXOS and NX-OS 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 Nexus 3600シリーズスイッチおよびCisco Nexus 9500 Rシリーズラインカードに影響を与えます。これらのスイッチでCisco NX-OSソフトウェアの脆弱性のあるリリースを実行していて、異なるAutonomous System(AS)値で設定された少なくとも1つのBGPネイバー（ピア）を持つBGP機能があり、次のシスコ製品IDのいずれかを持っている場合です。

- N3K-C36180YC-R
- N3K-C3636C-R
- N9K-X9624D-R2
- N9K-X9636C-R
- N9K-X9636C-RX
- N9K-X9636Q-R
- N9K-X96136YC-R

注：該当するCisco Nexus 3600シリーズスイッチ製品IDとCisco Nexus 9500 Rシリーズラインカード製品IDのリストは、このドキュメントの発行時点で正確でした。製品IDに関する具体的な質問については、Cisco Technical Assistance Center(TAC)にお問い合わせください。

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。

## BGPが有効になっているかどうかの確認

Cisco NexusデバイスにBGP機能とeBGPネイバーが設定されているかどうかを確認するには、show running-config | include "router bgp" と show running-config | include "neighbor"コマンドを使用して、Cisco NX-OSソフトウェアのCLIから機能が有効になっていることを確認します。

次の例は、Cisco NX-OSソフトウェアを実行しているデバイス上の1つのeBGPネイバーで有効になっているBGP機能を示しています。

```
<#root>

nxos-switch#

show running-config | include "router bgp"


router bgp 1
nxos-switch#

show running-config | include "neighbor"

neighbor 10.10.10.2 remote-as 2
```

### 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。

- 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
- MDS 9000 シリーズ マルチレイヤ スイッチ
- VMware vSphere 向け Nexus 1000 Virtual Edge
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- 「脆弱性が存在する製品」で言及されているモデル以外のNexus 3000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 6000 シリーズ スイッチ
- Nexus 7000 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
- 「脆弱性が存在する製品」で参照されているモデル以外の、スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ
- Cisco Secure Firewall 3100 シリーズ
- Cisco Secure Firewall 4200 シリーズ
- 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
- 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。

## 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 NX-OS ソフトウェア

お客様が Cisco NX-OS IOS 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 | |

## Nexus 3600シリーズスイッチおよびNexus 9500 Rシリーズラインカードの SMU

シスコはこの脆弱性に対処する次の SMU もリリースしています。次の SMU を Cisco.com の Software Center からダウンロードできます。

| Cisco NX-OS ソフトウェアリリース | Platform | SMU 名 |
|---|---|---|
| 9.3(12) | Nexus 3600 スイッチ<br>Nexus 9500 Rシリーズラインカード | nxos.CSCwh09703-n9k_ALL-1.0.0-9.3.12.lib32_n9000.rpm |
| 10.2(6) | Nexus 3600 スイッチ<br>Nexus 9500 Rシリーズラインカード | nxos64-msll.CSCwh09703-1.0.0-10.2.6.lib32_64_n9000.rpm |
| 10.3(4a) | Nexus 9500 Rシリーズラインカード[1] | nxos64-msll.CSCwh96478-1.0.0-10.3.4a.lib32_64_n9000.rpm |

1.リリース10.3(4a)を実行している場合は、N9K-X9636C-RXラインカードのみが該当します。他のすべてのモデルは、この特定のソフトウェアリリースでは影響を受けません。

Cisco Nexus 3600および9500スイッチ用のCisco NX-OSソフトウェアでのSMUのダウンロードと

インストールの詳細については、『Cisco Nexus 3000シリーズスイッチおよびCisco Nexus 9000シリーズスイッチ用のCisco NX-OSシステム管理設定ガイド』の「ソフトウェアメンテナンスアップグレードの実行」セクションを参照してください

### 関連情報

Cisco Nexus スイッチに最適な Cisco NX-OS ソフトウェアリリースの決定に際してサポートが必要な場合は、以下の推奨リリースに関するドキュメントを参照してください。セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザリのガイダンスに従うことをお勧めします。

Cisco MDS シリーズ スイッチ
VMware 向け Cisco Nexus 1000V スイッチ
Cisco Nexus 3000 Series Switches
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 5600 プラットフォームスイッチ
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 Series Switches
Cisco Nexus 9000 Series Switches
ACI モードの Cisco Nexus 9000 シリーズ スイッチ

Cisco UCS ソフトウェアに最適なリリースを確認するには、デバイスのリリースノートに記載されている推奨リリースに関するドキュメントを参照してください。

## 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-nxos-ebgp-dos-L3QCwVJ

## 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2月28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。