Cisco Nexus 3000および9000シリーズスイッチのBorder Gateway ProtocolにおけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-bgp-iefab-3hb2pwtx
初公開日 : 2026-05-20 16:00
バージョン 1.0 : Final
CVSSスコア : 6.8
回避策 : Yes
Cisco バグ ID : CSCwr23951

CVE-2026-20171

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

スタンドアロンNX-OSモードのCisco Nexus 3000シリーズスイッチおよびCisco Nexus 9000シリーズスイッチのBorder Gateway Protocol（BGP；ボーダーゲートウェイプロトコル）のenforce-first-as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BGPピアフラップをトリガーし、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、推移的なBGPアトリビュートの不適切な解析に起因します。攻撃者は、確立されたBGPピアセッションを介して巧妙に細工されたBGPアップデー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。アップデートが該当デバイスに伝搬されると、デバイスでBGPセッションがドロップされ、このアップデートを転送しているBGPピアでフラップが発生し、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。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-bgp-iefab-3hb2pwtx

該当製品

脆弱性のある製品

公開時点で、この脆弱性は、スタンドアロンNX-OSモードのCisco Nexus 3000シリーズスイッチおよびCisco Nexus 9000シリーズスイッチにBGPルーティングプロトコルが設定されている

場合に影響を与えました。

注：影響を受けるenforce-first-as機能は、BGPが設定されるとデフォルトで有効になり、デバイスの実行コンフィギュレーションには表示されません。この機能を無効にする方法については、このアドバイザリの「回避策」セクションを参照してください。

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。

デバイス設定の確認

デバイスでBGPピアリングセッションが確立されているかどうかを確認するには、show bgp sessionsコマンドを使用します。ルータがBGP用に設定されている場合、次の例に示すように、このコマンドはtotalとestablishedのピアを示す出力を返します。

<#root>

n9k#

show bgp sessions
Total peers 1, established peers 1

ASN 64550
VRF default, local ASN 64550
peers 1, established peers 1, local router-id 172.16.240.122
State: I-Idle, A-Active, O-Open, E-Established, C-Closing, S-Shutdown

Neighbor   ASN   Flaps LastUpDn|LastRead|LastWrit St Port(L/R) Notif(S/R)
10.0.0.2   64512 0   4d03h |00:00:36|00:00:32 E   24058/179   0/0

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、これら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、これらの脆弱性が次のシスコ製品に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
- 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
- Cisco Secure Firewall 200 シリーズ
- Cisco Secure Firewall 1200 シリーズ
- Cisco Secure Firewall 3100 シリーズ
- Cisco Secure Firewall 4200 シリーズ
- Cisco Secure Firewall 6100 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
- UCS 6600 シリーズ ファブリック インターコネクト
- UCS X シリーズ ダイレクト ファブリック インターコネクト 9108 100G

セキュリティ侵害の痕跡

この脆弱性の侵害の兆候は、ログのBGPネイバーフラッピングと不正なパスとして記録されるエラーメッセージです。次の例に示すように、log-neighbor-changesコンフィギュレーションコマンドを使用して、BGPネイバーの変更がログに記録されていることを確認します。

<#root>

```
router bgp 64550
```

log-neighbor-changes

最後の10個のログメッセージを表示するには、次の例に示すようにshow logging last 10コマンドを使用します。

<#root>

```
n9k# show logging last 10
2026 May 15 13:29:29 PE2 %BGP-5-ADJCHANGE:  bgp-2 [64512] (default) neighbor 10.0.0.2
```

Up

```
2026 May 15 13:29:30 PE2 %BGP-5-ADJCHANGE:  bgp-2 [64512] (default) neighbor 10.0.0.2
```

Down

```
 - sent:
```

malformed as path error

回避策

この脆弱性に対処する回避策は2つあります。該当デバイスがISPネットワーク全体でカスタマーエッジ(CE)属性を伝送するためにATTR_SET属性を使用する必要がない場合、RFC 6368では、この属性は省略可能で廃棄できると規定されています。

属性を廃棄して、アップデートに含まれるプレフィックスをルーティングテーブルに追加または更新するには、次の例のように、属性を送信しているネイバー設定でpath-attribute discard 128 in設定コマンドを追加します。

```
<#root>

router bgp 64550
  neighbor 10.0.0.2
    path-attribute discard 128 in
```

または、属性を破棄し、アップデートに含まれるプレフィックスをルーティングテーブルから削除するには、次の例のように、属性を送信しているネイバー設定でpath-attribute treat-as-withdraw 128 in設定コマンドを追加します。

```
<#root>

router bgp 64550
  neighbor 10.0.0.2
    path-attribute treat-as-withdraw 128 in
```

緩和策もあります。ATTR_SET属性を受信しているプロバイダーエッジ(PE)でenforce-first-asグローバルBGP機能を無効にするには、次の例に示すようにno enforce-first-asコマンドを設定します。これにより、最初の自律システム番号(ASN)チェックが無効になります。

```
<#root>

router bgp 64550
  no enforce-first-as
```

注：Cisco NX-OSソフトウェアのデフォルトのBGP動作を、この機能を無効にして変更すると、AS_PATHで予期しない最初の自律システム(AS)を受信した場合にBGPがピア隣接関係をダウンさせなくなり、セキュリティメカニズムが弱体化します。このポリシー変更を適用するには、BGPピアをリセットする必要があります。

これらの回避策と緩和策はすでに導入されており、テスト環境で効果を発揮することが実証されていますが、お客様の環境や使用条件下での適用性と有効性を確認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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

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 10.4(4)、ACI モードの Cisco NX-OS ソフトウェアの場合は 16.0(8e) 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

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
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 Cisco Technical Assistance Center（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-bgp-iefab-3hb2pwtx

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	2026年5月20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。