Cisco NX-OS ソフトウェアの Border Gateway Protocol におけるサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-20180620-nxosbgp

初公開日 : 2018-06-20 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 : CSCve79599 CSCve91387 CSCve91371 CSCve87784

CVE-2018-0295

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 Border Gateway Protocol（BGP）の実装における脆弱性により、認証されていないリモート攻撃者が、デバイスの予期しないリロードによるサービス妨害（DoS）状態を引き起こす可能性があります。

本脆弱性は、BGP アップデート メッセージの不完全な入力検証に起因しています。 細工された BGP アップデート メッセージがターゲット デバイスに送信されると、本脆弱性がエクスプロイトされる危険性があります。 エクスプロイトにより、スイッチの予期しないリロードが引き起こされる可能性があります。

BGP プロトコルのシスコの実装は、明示的に定義されているピアから受信する BGP トラフィックのみを受け入れます。 本脆弱性をエクスプロイトするために、攻撃者は、信頼できる BGP ピアからのものと見せかけた悪意のあるパケットを TCP 接続経由で送信するか、不正な形式のメッセージを被害者の BGP ネットワークに挿入できる必要があります。 このためには、該当システムの信頼ネットワーク内の BGP ピアに関する情報を取得することが必要です。

本脆弱性は、既存の BGP セッションでルータがピアから不正な形式の BGP メッセージを受信する際に生じる可能性があります。 ルータに脆弱性が生じるためには、少なくとも 1 つの BGP ネイバー セッションが確立されている必要があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-nxosbgp

このアドバイザリは、2018 年 6 月に公開された Cisco FXOS および NX-OS ソフトウェアのセキュリティ アドバイザリ コレクションの一部です。この中には、24 件の脆弱性に関する 24 件のシスコ セキュリティ アドバイザリが含まれています。 これらのアドバイザリとリンクの一覧については、以下を参照してください。Cisco Event Response: 2018 年 6 月 Cisco FXOS および NX-OS ソフトウェアのセキュリティ アドバイザリ コレクション

該当製品

脆弱性のある製品

本脆弱性は、Cisco NX-OS ソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えます。

- 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 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
- Nexus 7700 シリーズ スイッチ
- Nexus 9000 シリーズ ファブリック スイッチ（アプリケーション セントリック インフラストラクチャ（ACI）モード）
- スタンドアロン 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

脆弱性が存在する Cisco NX-OS 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」の項を参照してください。

NX-OS ソフトウェアの脆弱性の確認

本脆弱性は、BGP 機能が設定された NX-OS デバイスにのみ影響を与えます。 さらに、デバイスに少なくとも 1 つの BGP ネイバー（ピア）が設定されている必要があります。 悪意のある可能性がある BGP ピアが、NX-OS デバイス上に BGP ネイバーとして設定されている必要があります。 本脆弱性は、デバイス宛ての BGP のトラフィックに適用されます。 デバイスは、IP バージョン 4（IPv4）と IP バージョン 6（IPv6）の TCP ポート 179 で BGP パケットを処理します。

Nexus デバイスに BGP 機能と BGP ネイバーが設定されているかどうかを確認するには、管

理者が NX-OS CLI から **show running-config | include "router bgp"** と **show running-config | include "neighbor"** コマンドを使用して、機能が有効になっていることを確認します。

次の例は、NX-OS ソフトウェアを実行しているデバイスで BGP 機能が 1 つの BGP ネイバーとともに有効になっていることを示しています。

```
nxos-switch# show running-config | include "router bgp"
router bgp 64512
nxos-switch# show running-config | include "neighbor"
neighbor 209.165.201.1 remote-as 64497
```

Cisco 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 Cisco NX-OS ソフトウェアのリリースをチェックできます。 デバイスが Cisco NX-OS ソフトウェア リリース 7.3(2)D1(1) を実行している場合、コマンドの出力例は次のようになります。

```
nxos-switch# show version

Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
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 2.12.0
  kickstart: version 7.3(2)D1(1)
  system:    version 7.3(2)D1(1)
.
.
.
```

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 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 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
- 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

Cisco では、本脆弱性が Cisco Nexus 4000 シリーズ スイッチ、Cisco Nexus 5010 スイッチ、Cisco Nexus 5020 スイッチに影響するかどうかを調査していません。これらの製品がサポート終了ステータスに達しているためです。 詳細については、「IBM BladeCenter 用の Cisco Nexus 4000 シリーズ スイッチ モジュールの販売終了およびサポート終了通知」および「Cisco Nexus 5010 および Nexus 5020 スイッチの販売終了およびサポート終了通知」を参照してください。

回避策

この脆弱性に対処する回避策はありません。 ただし、MD5 による BGP ネイバー認証により、設定されている BGP ピアがスプーフィングされていないことを確認できます。

MD5 による BGP ネイバー認証の設定

MD5 ダイジェストを使用して、ピアからのルート アップデートを認証するように BGP を設定できます。 MD5 認証を使用するように BGP を設定するには、ネイバー コンフィギュレーション モード CLI で次のコマンドを使用します。

```
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
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 2.12.0
  kickstart: version 7.3(2)D1(1)
  system:    version 7.3(2)D1(1)
.
.
.
```

詳細については、『Cisco Nexus 7000 シリーズ NX-OS ユニキャスト ルーティング コンフィギュレーション ガイド』を参照してください。

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 アップデートを提供しています。 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.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、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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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 に連絡してアップグレードを入手してください。
http://www.cisco.com/en/US/support/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

この項の該当する表に示すように、適切なリリースにアップグレードすることをお勧めします。このアドバイザリはコレクションの一部です。これらも考慮した上、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。 コレクションに含まれるアドバイザリとリンクの一覧については、次を参照してください。シスコのイベント対応： 2018 年 6 月 Cisco FXOS および NX-OS ソフトウェアのセキュリティ アドバイザリ コレクション

次の表では、左の列に Cisco FXOS または NX-OS ソフトウェアのリリースを示しています。 中

央の列は、リリースがこのアドバイザリに記載されている脆弱性に該当するかどうか、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。 右の列は、リリースがこのアドバイザリ集に記載された何らかの脆弱性に該当するかどうか、および、それらすべて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。

Nexus 3000 シリーズ スイッチ： CSCve91387

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
7.0(3)I4 よりも前	7.0(3)I4(7)	7.0(3)I7(4)
7.0(3)I4	7.0(3)I4(7)	7.0(3)I7(4)
7.0(3)I5	7.0(3)I6(2)	7.0(3)I7(4)
7.0(3)I6	7.0(3)I6(2)	7.0(3)I7(4)
7.0(3)I7	脆弱性なし	7.0(3)I7(4)

Nexus 3500 プラットフォーム スイッチ： CSCve91371

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
6.0	6.0(2)A8(7)	7.0(3)I7(4)
7.0.3	7.0(3)I7(2)	7.0(3)I7(4)

Nexus 2000、5500、5600、6000 シリーズ スイッチ： CSCve79599

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
6.0	7.1(5)N1(1)	7.3(3)N1(1)
7.0	7.1(5)N1(1)	7.3(3)N1(1)
7.1	7.1(5)N1(1)	7.3(3)N1(1)
7.2	7.3(3)N1(1)	7.3(3)N1(1)
7.3	7.3(3)N1(1)	7.3(3)N1(1)

Nexus 7000 および 7700 シリーズ スイッチ CSCve79599

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
6.2	6.2(20)	8.1(2) または 8.2(1)
7.2	7.3(2)D1(1)	8.1(2) または 8.2(1)
7.3	7.3(2)D1(1)	8.1(2) または 8.2(1)
8.0	8.1(2)	8.1(2) または 8.2(1)
8.1	8.1(2)	8.1(2) または 8.2(1)
8.2	8.2(1)	8.1(2) または 8.2(1)

ACI モードの Nexus 9000 シリーズ ファブリック スイッチ： CSCve87784

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
12.1/2.1 よりも前	12.1(3h)/2.1(3h)	13.1(1i)/3.1(1i)
12.1/2.1	12.1(3h)/2.1(3h)	13.1(1i)/3.1(1i)
12.2/2.2	12.2(3j)/2.2(3j)	13.1(1i)/3.1(1i)
12.3/2.3	13.0(1k)/3.0(1k)	13.1(1i)/3.1(1i)
13.0/3.0	13.0(1k)/3.0(1k)	13.1(1i)/3.1(1i)
13.1/3.1	脆弱性なし	13.1(1i)/3.1(1i)

スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ： CSCve91387

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
7.0(3)I4 よりも前	7.0(3)I4(7)	7.0(3)I7(4)
7.0(3)I4	7.0(3)I4(7)	7.0(3)I7(4)
7.0(3)I5	7.0(3)I6(2)	7.0(3)I7(4)
7.0(3)I6	7.0(3)I6(2)	7.0(3)I7(4)
7.0(3)I7	脆弱性なし	7.0(3)I7(4)

Nexus 9500 R シリーズ向けライン カードおよびファブリック モジュール、Nexus 3600 プラットフォーム スイッチ: CSCve79599

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
7.0	7.0(3)F2(2)	7.0(3)F3(3a)

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

本脆弱性は、TAC のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-nxosbgp

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018 年 6 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。