Cisco IOS XR ソフトウェアの BGP MPLS-Based EVPN で確認されたサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20190515-iosxr-evpn-dos
初公開日 : 2019-05-15 16:00
最終更新日 : 2019-07-10 16:56
バージョン 1.1 : Final
CVSSスコア : 7.4
回避策 : No workarounds available
Cisco バグ ID : CSCvk35997

CVE-2019-1849

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 ソフトウェアに実装されたボーダー ゲートウェイ プロトコル（BGP）のマルチプロトコル ラベル スイッチング（MPLS）ベースのイーサネット VPN（EVPN）で脆弱性が確認されました。認証されていない攻撃者が、隣接するネットワークから標的デバイスにサービス妨害（DoS）を仕掛ける危険性があります。

この脆弱性は、影響を受けるソフトウェアが特定のプロセスを実行するときに発生する論理エラーに起因します EVPN ルーティング情報.悪意のあるトラフィック パターンをターゲットの EVPN ネットワークに注入することでエクスプロイトされる可能性があります。

エクスプロイトに成功すると、同じ EVPN インスタンス（EVI）のプロバイダー エッジ（PE）デバイス メンバー上で、l2vpn_mgr プロセスがクラッシュする恐れがあります。対象となるデバイスでクラッシュが発生するとシステムが不安定になるため、デバイスからのトラフィック処理および転送が不可能となり、DoS 状態に陥る危険性があります。通常の運用状態を復元するためには、手動による介入が必要です。

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-20190515-iosxr-evpn-dos

該当製品

脆弱性のある製品

この脆弱性の影響を受けるのは、シスコ デバイスで脆弱性が存在する Cisco IOS XE ソフトウェア リリースが稼働し、BGP MPLS ベースの EVI を使用している場合です。

シスコでは、この脆弱性が Cisco IOS XR 32 ビット ソフトウェアと Cisco IOS XR 64 ビット ソフトウェアの両方に影響を与えることを確認しました。

脆弱性が存在する Cisco IOS XR ソフトウェア リリースの詳細については、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。

デバイスの設定に脆弱性があるかどうかの確認

デバイスの設定に脆弱性があるかどうかを確認するには、2 通りの方法があります。

オプション1:show evpn eviの使用 | include EVPN コマンド

管理者は show evpn evi を使用できます。 | include EVPN コマンドを実行すると、デバイスで BGP MPLS ベースの EVI が使用されているかどうかを判断できます。

以下は、BGP MPLS ベースの EVI を使用しているデバイスに対してコマンドを実行した場合の出力例です。

```
<#root>

RP/0/0/CPU0:Router#

show evpn evi | i EVPN

Tue May 14 09:40:09.277 EST
```

```
<#root>

VPN-ID     Encap     Bridge Domain                 Type
---------- ------ ---------------------------- -------------------
<VPN-ID>   MPLS     <BD-NAME>

EVPN
```

このコマンドが存在しない場合、または出力のタイプ列内に EVPN の文字列が表示されない場合、そのデバイスはこのアドバイザリで説明されている脆弱性の影響を受けません。

オプション2:show running-config formal l2vpn | include "l2vpn bridge group [^]+ bridge-domain [^]+ evi [0-9]+" コマンド

管理者は、show running-config formal l2vpn を使用できます。 | include "l2vpn bridge group [^] + bridge domain [^] + evi [0-9] +" コマンドを実行すると、BGP MPLS ベースの EVI がデバイスで使用されているかどうかを判断できます。以下は、BGP MPLS ベースの EVI を使用しているデバイスに対してコマンドを実行した場合の出力例です。

```
<#root>

RP/0/0/CPU0:Router#

show running-config formal l2vpn | include "l2vpn bridge group [^ ]+ bridge-domain [^ ]+ evi [0-9]+"

l2vpn bridge group

             bridge-domain

              evi
```

このコマンドによる出力がないの場合、デバイスはこのアドバイザリで説明されている脆弱性の影響を受けません。

注：ハードウェアとソフトウェアの組み合わせによっては、show running-config formalコマンドをサポートしていない場合があります。その場合は、オプション 1 で示されている確認手順を使用します。

Cisco IOS XR ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS XR ソフトウェア リリースとそれを実行しているデバイスの名前は、管理者がデバイスにログインして、CLI で show version コマンドを使用することにより確認できます。デバイスで Cisco IOS XR ソフトウェアが稼働している場合、システム バナーに Cisco IOS XR Software といったテキストが表示されます。デバイスで現在実行しているシステム イメージ ファイルの場所と名前は、「System image file is」の横に表示されます。ハードウェア製品の名前はシステム イメージ ファイル名の次の行に表示されます。

以下は、Cisco IOS XR ソフトウェア リリース 6.5.2 が稼働中のデバイスで show version command コマンドを実行した場合の出力例です。

```
<#root>

RP/0/RSP0/CPU0:ASR9001#

show version

Tue May 14 01:32:32.751 EST

Cisco IOS XR Software, Version

6.5.2

[Default]
Copyright (c) 2019 by Cisco Systems, Inc.

ROM: System Bootstrap, Version 2.04(20140227:092320) [ASR9K ROMMON],

ASR9001 uptime is 6 hours, 17 minutes
System image file is "bootflash:disk0/asr9k-os-mbi-5.3.4.sp4-1.0.0/0x100000/mbiasr9k-rp.vm"

cisco ASR9K Series (P4040) processor with 8388608K bytes of memory.
P4040 processor at 1500MHz, Revision 2.0
ASR-9001 Chassis

2 Management Ethernet
8 TenGigE
20 GigabitEthernet
8 DWDM controller(s)
8 WANPHY controller(s)
44 GigabitEthernet/IEEE 802.3 interface(s)
219k bytes of non-volatile configuration memory.
2880M bytes of hard disk.
3932144k bytes of disk0: (Sector size 512 bytes).

Configuration register on node 0/RSP0/CPU0 is 0x2102
```

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。

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

シスコでは、この脆弱性が Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、Cisco NX-OS ソフトウェアが稼働しているデバイスに影響を与えないことを確認しました。

詳細

EVPN は、MPLS ネットワーク上でイーサネット マルチポイント サービスを提供する次世代ソリューションです。EVPN では、顧客の MAC アドレスがルーティング可能なアドレスとして使用されます。EVI に対応した PE デバイスでは、ルートの学習および分散メカニズムとして、マルチプロトコル BGP（MP-BGP）が使用されます。

この脆弱性は、対象となるソフトウェアが特定の MP-BGP EVPN アップデート メッセージを処理するときに発生する論理エラーに起因します。複数のカスタマーエッジ（CE）デバイスを制御する攻撃者は、悪意のあるトラフィックパターンを EVPN ネットワークに注入することで、この脆弱性をエクスプロイトする危険性があります。エクスプロイトによって、プロバイダー エッジ（PE）デバイスで特定の MP-BGP EVPN アップデート メッセージをアドバタイズされ、その結果、同じ EVI の PE デバイス メンバーで l2vpn_mgr プロセスがクラッシュする恐れがあります。

セキュリティ侵害の痕跡

この脆弱性がエクスプロイトされると、該当デバイスで、次のようなエラー メッセージが繰り返し生成される可能性があります。

```
RP/0/RP0/CPU0:May 14 15:41:03.241 IST: syslog_dev[117]: l2vpn_mgr[1265] PID-8642:
l2vpn/evpn/include/evpn_label_db_defs.h: 412 FALSE -- assertion failed
```

脆弱性のエクスプロイトによってデバイスが影響を受けているかどうかを判断するには、サポート担当部門に連絡し、エラーメッセージの調査をご依頼ください。

回避策

この脆弱性に対処する回避策はありません。

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

次の表では、Cisco IOS XR ソフトウェアの主なソフトウェア リリース トレインを記載します。本アドバイザリで説明されている脆弱性によるリリース トレインへの影響の有無、また影響を受ける場合の修正を含む最初のマイナー リリースを記載します。次の表に示すように、適切なリリースに移行する必要があります。

ソフトウェア トレイン	First Fixed Release（修正された最初のリリース）	推奨リリース
4.3	脆弱性なし	脆弱性なし
5.0	脆弱性なし	脆弱性なし
5.1	脆弱性なし	脆弱性なし
5.2	脆弱性なし	脆弱性なし
5.3	脆弱性なし	脆弱性なし
6.0	脆弱性なし	脆弱性なし
6.1	6.5.3	6.5.3
6.2	6.5.3	6.5.3
6.3	6.3.3	6.3.3
6.4	6.4.2	6.4.2

6.5	6.5.2	6.5.3
6.6	6.6.1	6.6.12

シスコでは、この脆弱性に対処する Cisco アグリゲーション サービス ルータ（ASR）9000 シリーズ向けのソフトウェア メンテナンス アップグレード（SMU）もリリースしています。

IOS XR リリース	SMU ID	ASR 9000 SMU 名
6.2.3	AA15558	asr9k-px-6.2.3.CSCvk35997

SMU やサービス パックは、Cisco.com の Software Center からダウンロードできます。

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

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-20190515-iosxr-evpn-dos

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	SMU 情報を追加しました。	修正済みソフトウェア	Final	2019 年 7 月 10 日
1.0	初回公開リリース	—	Final	2019 年 5 月 15 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。