Cisco IOS XE ソフトウェア イーサネット バーチャル プライベート ネットワーク ボーダゲートウェイ・ プロトコル サービス拒否の脆弱性

Medium

アドバイザリーID : cisco-sa-20171103-bgp

初公開日 : 2017-11-03 16:00

最終更新日 : 2017-11-07 19:28

バージョン 1.1 : Final

CVSSスコア : 6.8

回避策 : No workarounds available

Cisco バグ ID : CSCvg52875 CSCui67191

CVE-2017-12319

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 XE ソフトウェアのためのイーサネット バーチャル プライベート ネットワーク（EVPN）上のボーダー ゲートウェイ プロトコル（BGP）の脆弱性は、サービス拒否（DoS）状態に終って、または可能性としては破損したネットワークの不安定性という結果に終る可能性がある BGPルーティングテーブル リロードします非認証、リモート攻撃者によりデバイスはことを可能にする可能性があります。

IOS XE ソフトウェア リリース間の BGP MPLS ベース イーサネット VPN RFC（RFC 7432）草案の実装の変更による脆弱性存在。 BGP 含んだマルチキャスト イーサネット タグ ルートまたは BGP EVPN MAC/IP アドバタイズメントはアップデートパケット受け取られるとき、IP アドレス長フィールドが誤算されることは可能性のあるである可能性があります。 攻撃者は影響を受けたデバイスへ巧妙に細工された BGP パケットを送信 することによって BGPセッションが設定された後この脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者により影響を受けたデバイスは BGPルーティングテーブルをリロードするか、または破損しますことを可能にする可能性があります; どちらかの結果は DoS という結果に終ります。

BGP プロトコルの Ciscoインプリメンテーションは明示的に定義されたピアからの着信 BGP トラフィックだけを受け入れます。 この脆弱性を不正利用するために、攻撃者は対象の BGPネットワークに信頼された BGPピアから来るようであるまたはインジェクトします不正メッセージを必要があります TCP 接続上の悪質なパケットを送信できる。 これは影響を受けたシステムの信

頼できるネットワークの BGPピアについての情報の取得を必要とします。

脆弱性はルータが既存の BGPセッションのピアから巧妙に細工された BGP メッセージを受け取るとき引き起こされるかもしれません。 少なくとも 1 つの BGP 隣接セッションはルータが脆弱であることができるように設定する必要があります。

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-20171103-bgp

該当製品

脆弱性のある製品

この脆弱性はソフトウェア リリース 16.3 前に BGP EVPN 設定をサポートする Cisco IOS XE ソフトウェアのすべてのリリースに該当します。 デバイスが EVPN のために設定されない場合、脆弱ではないです。

Cisco IOS XE 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 XE ソフトウェア リリースは、管理者がデバイスにログインして、CLI で **show version コマンド**を実行し、表示されるシステム バナーを参照することにより確認できます。 デバイスが Cisco IOS XE ソフトウェアを実行する場合、システム バナーは *Cisco IOSソフトウェア*、 *Cisco IOS XE ソフトウェア*、または同じようなテキストを表示します。

次の例は Cisco IOS XE ソフトウェア リリース 16.2.1 を実行して、 *CAT3K_CAA-UNIVERSALK9-M* のインストール済みイメージ名前があるデバイスのためのコマンドの出力を示したものです:

```
ios-xe-device# show version

Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali
16.2.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 by mcpre
.
.
.
```

Cisco IOS XE ソフトウェア リリースの命名と番号付けの規則については、以下を参照してください。 ホワイト ペーパー： Cisco IOS および NX-OS ソフトウェア リファレンス ガイド
EVPN 設定のその他の情報に関しては、 キャリア イーサネットコンフィギュレーション ガイドを参照して下さい。

脆弱性を含んでいないことが確認された製品

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。

Cisco はこの脆弱性が Cisco IOS XR ソフトウェアおよび Cisco NX-OS ソフトウェアに影響を与えないことを確認しました。

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 アップデートを提供しています。 Cisco は利用可能になると同時に該当するリリースに修正を提供し続けます。

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。

Cisco IOS XE ソフトウェア

この脆弱性は IOS XE ソフトウェアリリース 16.3 およびそれ以降で解決されます。

顧客が Cisco IOS XE ソフトウェアの脆弱性への公開を判別するのを助けるために Cisco はツールを、特定のソフトウェア リリースおよび諮問それぞれに説明がある脆弱性を解決する以前のリリースに影響を与える Cisco Security Advisory を識別する Cisco IOSソフトウェア チェッカー提供します、（「最初に」固定される）。 また該当する場合、すべてのアドバイザリに記載された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。

このツールを使用して次のタスクを実行できます。

- ドロップダウン メニューからリリース（複数可）を選択するか、分析対象となるローカル システムからファイルをアップロードして、検索を開始する
- show version コマンドの出力をツールで解析する
- カスタマイズした検索（過去に公開されたすべてのシスコ セキュリティ アドバイザリを検索対象に含めたり、特定のアドバイザリのみ、または最新のバンドル資料から全アドバイザリを含めるなど）を作成する

リリースがあらゆる公開された Cisco Security Advisory から影響を受けするかどうか判別するために、Cisco.com の Cisco IOSソフトウェア チェッカーを使用するか、または—次のフィールド

で… Cisco IOS XE ソフトウェア リリースを—たとえば、**15.1(4)M2** 入力して下さい:

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

この脆弱性は Cisco TAC ケースによって顧客によって Cisco に報告されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171103-bgp

改訂履歴

Version	Description	Section	Status	日付
1.1	第 2 Ciscoバグ 識別子を追加しました: CSCui67191.	製品特質セット	Final	2017-November-07
1.0	初回公開リリース		Final	2017 11 月 3 日

利用規約