Cisco Catalyst 4000 シリーズ スイッチで確認された TCP サービス妨害（DoS）の脆弱性

アドバイザリーID : cisco-sa-20190925-cat4000-tcp-dos
CVE-2019-12652
初公開日 : 2019-09-25 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 : CSCvk66730

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 Catalyst 4000 シリーズ スイッチ向け Cisco IOS ソフトウェアの入力パケット処理機能で脆弱性が確認されました。認証されていないリモートからの攻撃者によって、標的デバイスでサービス妨害（DoS）状態が引き起こされる危険性があります。

この脆弱性は、特定の Cisco Catalyst 4000 シリーズ スイッチで、デバイスに送信される TCP パケットを処理する際のリソース割り当てが不適切であることに起因します。細工した TCP ストリームを標的デバイスに送信することで、この脆弱性が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、標的デバイスでバッファ リソースが使い果たされて、コントロール プレーン プロトコルと管理プレーン プロトコルの動作が損なわれるため、DoS 状態に陥る危険性があります。

この脆弱性は、該当デバイスを宛先とするトラフィックによってのみトリガーされ、該当デバイスを通過するトラフィックを使用してエクスプロイトされることはありません。

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-20190925-cat4000-tcp-dos

このアドバイザリは、2019 年 9 月 25 日に公開された Cisco IOS および IOS XE ソフトウェア リリースのセキュリティ アドバイザリ資料の一部です。この資料には、13 件の脆弱性に関する 12 件のシスコ セキュリティ アドバイザリが記載されています。アドバイザリとリンクの一覧については、『Cisco Event Response: September 2019 Semiannual Cisco IOS and IOS XE 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

この脆弱性の影響を受けるのは、次のデバイスで脆弱性のある Cisco IOS ソフトウェア リリースを稼動している場合です。

- Cisco Catalyst 4500 Supervisor Engine 6-E
- Cisco Catalyst 4500 Supervisor Engine 6L-E
- Cisco Catalyst 4900M スイッチ
- Cisco Catalyst 4948E イーサネット スイッチ
- Cisco Catalyst 4948E-F イーサネット スイッチ

公開時点で脆弱性が確認されている Cisco IOS 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。

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 Cisco IOS XE ソフトウェア、Cisco IOS XR ソフトウェア、Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

詳細

この脆弱性がエクスプロイトされると、標的デバイスのバッファ リソースが枯渇する可能性があります。これにより、デバイス宛てのユニキャスト IP パケットを受信して処理できなくなることがあります。その結果、BGP ルーティング プロトコルなどのユニキャスト IP トラフィックに依存する管理プロトコルとコントロール プレーン プロトコルが、標的デバイスで正常な動作を停止し、DoS 状態に陥る危険性があります。

この脆弱性は、細工した TCP ストリームを IPv4 または IPv6 経由で使用することで、エクスプロイトされる可能性があります。この脆弱性は、該当デバイスを宛先とする TCP トラフィックによってのみトリガーされ、該当デバイスを通過するトラフィックを使用してエクスプロイトされることはありません。

この脆弱性をエクスプロイトするには、攻撃者は該当デバイスの開いている TCP ポートへの TCP 接続を確立する必要があります。結果として、スプーフィングされた IP アドレスを使用して攻撃を実行することはできません。

回避策

この脆弱性に対処する回避策はありません。

『Cisco IOS デバイスの強化ガイド』で推奨されているように、インフラストラクチャ アクセス コントロール リスト（iACL）と vty ACL を使用すれば、確実に信頼できる送信元 IP アドレスからのアクセスだけを許可して攻撃対象領域を縮小することが可能です。

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。

Cisco IOS ソフトウェア

お客様が Cisco 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、シスコでは Cisco IOS Software Checker ツールを提供しています。このツールにより、特定の Cisco IOS ソフトウェア リリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。また該当する場合、そのリリースに関するすべてのアドバイザリ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 リストからリリース（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入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべてのアドバイザリを含めるなど）を作成する

リリースが、公開されたシスコセキュリティアドバイザリのいずれかに該当するかどうかを確認するには、Cisco.comのCisco IOS Software Checkerを使用するか、次のフィールドにCisco IOSソフトウェアリリース(たとえば、15.1(4)M2)を入力します。

Check

デフォルトでは、Cisco IOS ソフトウェアのチェックには、結果は、高セキュリティへの影響の評価 (サー) または重大な脆弱性にのみが含まれています。「中間」の SIR 脆弱性の結果を含めるには、Cisco.com の Cisco IOS ソフトウェア チェッカーを使用して、[Impact Rating] ドロップダウン リストの [中間（Medium）] チェックボックスをオンにします。

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

この脆弱性を報告していただいた Akamai 社の Tim April 氏、Trevers Astheimer 氏、Aaron Block 氏、John-Nicholas Furst 氏、および Eric Kloster 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-cat4000-tcp-dos

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2019 年 9 月 25 日

利用規約

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。