Cisco StarOS 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-20190619-staros-asr-dos

初公開日 : 2019-06-19 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 : CSCvn06757

CVE-2019-1869

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

仮想プラットフォームで実行される Cisco StarOS オペレーティング システムの内部パケット処理機能に存在する脆弱性により、認証されていないリモートの攻撃者が、該当デバイスでトラフィック処理を停止させ、サービス妨害（DoS）状態を引き起こす恐れがあります。

この脆弱性は、特定のトラフィック条件で発生する可能性がある論理エラーに起因します。攻撃者は、細工された一連のパケットを該当デバイスに送信することにより、この脆弱性を エクスプロイトする危険性があります。不正利用に成功すると、攻撃者は、標的にしたサービス インターフェイスでトラフィックを受信できないようにする可能性があります。これにより、該当のインターフェイスで DoS 状態が発生します。

この脆弱性のエクスプロイトから回復するために、手動によるデバイスのリロードが必要になる場合があります。

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。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-20190619-staros-asr-dos

該当製品

脆弱性のある製品

この脆弱性は、Cisco StarOS オペレーティング システムの脆弱性のあるバージョンを実行する次のシスコ製品に影響を与えます。

- Cisco Virtualized Packet Core-Single Instance（VPC-SI）
- Cisco Virtualized Packet Core-Distributed Instance（VPC-DI）

脆弱性が存在する Cisco StarOS 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、Cisco ASR 5000 シリーズ アグリゲーション サービス ルータがこの脆弱性の影響を受けないことを確認済みです。

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

このセクションの表を参考に、適切な修正済みリリースにアップグレードする必要があります。次の表の最初の列に Cisco StarOS オペレーティング システムのメジャー リリースを、2 番目の列に、脆弱性のある最初のバージョンをメジャー リリースごとに示します。また、3 番目の列に、この脆弱性に対する修正が含まれる最初のリリースを示します。

Cisco StarOS Major Release	脆弱性のある最初のリリース	First Fixed Release（修正された最初のリリース）
21.6 より前	脆弱性なし	脆弱性なし
21.6	21.6.12	21.6.13
21.6b	21.6b.13	21.6b.16
21.7	21.7.8	21.7.11
21.8	21.8.6	21.8.10
21.9	21.9.2	21.9.7
21.10	21.10.0	21.10.2
21.11	21.11.0	21.11.1
21.12	脆弱性なし	脆弱性なし

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-20190619-staros-asr-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 6 月 19 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。