# Cisco IOS XEソフトウェアのAppNav-XEにおけるDoS脆弱性


アドバイザリーID : cisco-sa-appnav-xe-dos-j5MXTR4
初公開日 : 2022-04-13 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 : CSCvx26652

CVE-2022-20678

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AppNav-XE機能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該当デバイスのリロードを引き起こし、その結果、サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、特定のTCPセグメントの不適切な処理に起因します。攻撃者は、該当デバイスのインターフェイスを介して、巧妙に細工されたTCPトラフィックのストリームを高速で送信することで、この脆弱性を不正利用する可能性があります。このインターフェイスでは、AppNav代行受信を有効にする必要があります。エクスプロイトに成功すると、攻撃者は標的デバイスのリロードを引き起こすことができるようになります。

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-appnav-xe-dos-j5MXTR4

このアドバイザリは、2022 年 4 月に公開された Cisco IOS ソフトウェアおよび 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 バンドルの一部です。アドバイザリの完全なリストとそのリンクについては、『Cisco Event Response: April 2022 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication Publication』を参照してください。

## 該当製品

## 脆弱性のある製品

この脆弱性は、Cisco IOS XEソフトウェアの脆弱性が存在するリリースを実行し、AppNav-XE機能が有効になっている次のシスコ製品に影響を与えます。

- 1000 シリーズ サービス統合型ルータ
- 4000 シリーズ サービス統合型ルータ
- ASR 1001-Xルータ
- ASR 1002-Xルータ
- Catalyst 8300シリーズルータ
- Catalyst 8500シリーズルータ
- Catalyst 8000V エッジソフトウェア
- Cloud Services Router 1000V シリーズ

注：Cisco IOS XEソフトウェアでは、AppNav-XE機能はデフォルトで無効になっています。

脆弱性が存在する Cisco 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。

## AppNav-XE設定の確認

AppNav-XEの設定を確認するには、まず次の条件がすべて満たされていることを確認します。

- 少なくとも1つのインターフェイスでAppNavインターセプションが有効になっています
- AppNav Controllerグループが構成されており、少なくとも1つのAppNav Controllerメンバーを持っています
- サービスノードグループが構成され、少なくとも1つのサービスノードメンバーを持つ
- タイプwaasのサービスコンテキストが設定され、有効になり、AppNavコントローラグループ、サービスノードグループ、およびサービスポリシーにリンクされます

AppNavインターセプションが少なくとも1つのインターフェイスで有効になっているかどうかを確認するには、次のいずれかのオプションを使用します。

- 適用されたコマンドとマクロ名を表示するには、show running-config | include ^interface|service-insertion waas CLIコマンドを使用して、service-insertion waasが少なくとも1つのインターフェイスで設定されていることを確認します。次の例は、インターフェイスGigabitEthernet1でAppNavインターセプションが有効になっているデバイスでの出力を示しています。

```
<#root>

Router#

show running-config | include ^interface|service-insertion waas
```

```
interface VirtualPortGroup0
interface GigabitEthernet1

service-insertion waas

interface GigabitEthernet2
Router#
```

- show service-insertion status | appnav Enabled Interfaces CLIコマンドを開始し、結果の出力に少なくとも1つのインターフェイスがリストされていることを確認します。次の例は、インターフェイスGigabitEthernet1でAppNav-XE機能が有効になっているデバイスでの出力を示しています。

```
<#root>

Router#

show service-insertion status | begin AppNav Enabled Interfaces

AppNav Enabled Interfaces:

GigabitEthernet1

Router#
```

AppNav Controllerグループ、サービスノードグループ、およびwaasタイプのサービスコンテキストが設定されていて有効になっているかどうかを確認するには、show running-config | セクションservice-insertion CLIコマンドを使用します。次の例は、すべての要件を満たすデバイスでの出力を示しています。

```
<#root>

Router#

show running-config | section service-insertion

service-insertion service-node-group

 WNG-Default-1

service-node

 192.168.100.102
 service-node 192.168.100.2

service-insertion appnav-controller-group

 scg
```

```
appnav-controller
 192.168.10.10
service-insertion service-context waas
/1

appnav-controller-group
 scg

service-node-group
 WNG-Default-1

service-policy
 APPNAV-1-PMAP
 vrf default

enable



service-insertion waas

Router#
```

### 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。

- Cisco Wide Area Application Services(WAAS)ソフトウェアを実行するAppNavコントローラ
- IOS ソフトウェア
- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア

## 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。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

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。

Cisco.com の Cisco Support and Downloads ページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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 セキュリティ アドバイザリ 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アップグレード ソリューション一式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（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

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 および IOS XE ソフトウェア

Cisco IOS ソフトウェアおよび IOS XE 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 Software Checker を提供しています。このツールにより、特定の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。

お客様は、Cisco Software Checker を使用して次の方法でアドバイザリを検索できます。

- ソフトウェアと 1 つ以上のリリースを選択します。
- 特定のリリースのリストを含む .txt ファイルをアップロードする
- show version コマンドの出力を入力する

検索を開始した後で、すべてのシスコ セキュリティ アドバイザリ、特定のアドバイザリ、または最新の公開資料に記載されているすべてのアドバイザリが含まれるように検索をカスタマイズできます。

また、次の形式を使用して、Cisco IOS または IOS XE ソフトウェアリリース（15.1(4)M2 や 3.13.8S など）を入力することで、そのリリースがシスコ セキュリティ アドバイザリの影響を受けているかどうかを判断できます。

Check

デフォルトでは、Cisco Software Checker の結果には、Security Impact Rating（SIR）が「重大」または「高」の脆弱性だけが含まれます。「中間」の SIR 脆弱性の結果を含めるには、Cisco.com にある Cisco Software Checker を使用して、検索をカスタマイズするときに [影響の評価（Impact Rating）] の下にある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

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appnav-xe-dos-j5MXTR4

## 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 | 2022年 4 月 13 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。