Cisco IOx Application Hosting EnvironmentのDoS脆弱性

Medium

アドバイザリーID : cisco-sa-iox-dos-95Fqnf7b
初公開日 : 2025-05-07 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : No workarounds available
Cisco バグ ID : CSCwj81278

CVE-2025-20196

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ソフトウェアおよびCisco IOS XEソフトウェアのCisco IOxアプリケーションホスティング環境における脆弱性により、認証されていないリモートの攻撃者がCisco IOxアプリケーションホスティング環境の応答を停止させ、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、HTTP要求の不適切な処理に起因します。攻撃者は、該当デバイスに巧妙に細工された HTTP 要求を送信することにより、この脆弱性をエクスプロイトすることができます。エクスプロイトに成功すると、攻撃者はCisco IOxアプリケーションホスティング環境の応答を停止させることができます。サービスを回復するには、IOxプロセスを手動で再起動する必要があります。

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-iox-dos-95Fqnf7b

このアドバイザリは、2025年5月に公開されたCisco IOSソフトウェアおよびIOS XEソフトウェアのセキュリティアドバイザリバンドルの一部です。これらのアドバイザリとリンクの一覧については、『シスコイベントレスポンス：Cisco IOSおよびIOS XEソフトウェアに関するセキュリティアドバイザリ公開資料（半年刊、2025年5月）』を参照してください。

該当製品

脆弱性のある製品

公開時点では、Cisco IOSおよびIOS XEソフトウェアがCisco IOxアプリケーションホスティング環境で設定されており、HTTPサーバ機能が有効になっている場合、この脆弱性の影響を受けます。Cisco IOxアプリケーションホスティング環境は、デフォルトでは有効になっていません。

この脆弱性は、公開時点で次のシスコ製品にも影響を与えました。

- 800 シリーズ産業用 ISR
- Catalyst 9100ファミリのアクセスポイント(COS-AP)
- CGR1000コンピューティングモジュール
- IC3000産業用コンピューティングゲートウェイ
- IR510 WPAN 産業用ルータ

このアドバイザリの公開時点で脆弱性が存在するシスコ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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

IOxアプリケーションホスティング環境が有効になっているかどうかの確認

オプション1:show iox-service CLIコマンドを使用します。

IOx機能のステータスを確認するには、次の例に示すように特権EXECモードでshow iox-serviceコマンドを使用します。

<#root>

```
Router#
show iox-service

IOx Infrastructure Summary:
---------------------------
IOx service (CAF)          :
Running

IOx service (HA)           : Running
IOx service (IOxman)       : Running
Libvirtd                   : Running
```

IOxサービス(CAF)がRunning状態である場合、デバイスはこの脆弱性の影響を受ける可能性があります。「HTTPサーバ設定の判別」に進みます。

次の条件のいずれかが当てはまる場合、そのデバイスはこの脆弱性の影響を受けません。

- IOxサービス(CAF)がNot Running状態である。
- show iox-service特権EXECモードコマンドを使用しても出力が返されません。
- show iox-service特権EXECモードコマンドを使用すると、エラーが返されます。

オプション 2：iox 構成コマンドを使用する.

代替策として、次の例に示すように、実行コンフィギュレーションでioxコンフィギュレーションコマンドを確認します。

```
<#root>

Router#

sh run | include iox

iox
```

例に示すように、出力にioxだけの行が含まれている場合、そのデバイスはこの脆弱性の影響を受ける可能性があります。「HTTPサーバ設定の判別」に進みます。

ioxコンフィギュレーションコマンドが出力を返さない場合、またはエラーが返される場合、そのデバイスはこの脆弱性の影響を受けません。

HTTP サーバ設定の確認

HTTPサーバ機能がデバイスで有効になっているかどうかを確認するには、デバイスにログインし、CLIでshow running-config | include ip http server|secure|activeコマンドを使用して、グローバルコンフィギュレーションにip http serverコマンドまたはip http secure-serverコマンドが存在するかどうかを確認します。どちらかのコマンドが含まれている場合は、HTTP サーバー機能が有効です。

次の例は、HTTPサーバ機能が有効になっているデバイスでのshow running-config | include ip http server|secure|activeコマンドの出力を示しています。

```
<#root>

Router#

show running-config | include ip http server|secure|active


ip http server
ip http secure-server
```

注：デバイス設定にどちらかのコマンドまたは両方のコマンドが含まれている場合は、Web

UI機能が有効になっています。

ip http server コマンドが存在し、設定に ip http active-session-modules none が含まれている場合、脆弱性が HTTP 経由でエクスプロイトされることはありません。

ip http secure-serverコマンドが存在し、設定にip http secure-active-session-modules noneも含まれている場合、この脆弱性はHTTPSでは不正利用できません。

IOxアプリケーション環境の復元

Cisco IOxアプリケーションホスティング環境は、ユーザの介入なしには回復しません。次の例に示すように、no ioxコマンドとioxコンフィギュレーションコマンドを使用して再起動する必要があります。

```
<#root>

Router(config)#

no iox


Router(config)#

iox
```

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

回避策

この脆弱性に対処する回避策はありません。

ただし、緩和策があります。Cisco IOxアプリケーションホスティング環境を必要としないお客様は、no ioxコンフィギュレーションコマンドを使用して、デバイスのCisco IOxを無効にすることを推奨します。Cisco IOxホスティング環境が必要な場合は、no ip http serverおよびno ip http secure-serverコンフィギュレーションコマンドを使用してHTTPサーバを無効にすることができます。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環

境への適用性と環境への影響を評価した後で導入してください。

修正済みソフトウェア

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。

修正済みリリース

発行時点では、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左側の列には、該当するシスコプラットフォームが表示されます。右側の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

シスコ プラットフォーム	First Fixed Release（修正された最初のリリース）
800 シリーズ産業用 ISR	15.9(3)M11
Catalyst 9100ファミリのアクセスポイント(COS-AP)	17.15.2
CGR1000コンピューティングモジュール	15.9(3)M12（2025年8月）
IC3000産業用コンピューティングゲートウェイ	1.5.2
IOS XEベースのデバイスでIOxが設定されている	17.9.7 17.12.5 17.15.3 17.16.1 詳細については、次のセクションのCisco IOSおよびIOS XEソフトウェアチェッカーを参照してください
IR510 WPAN 産業用ルータ	今後のリリース

シスコの Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正済

みリリース情報のみを検証します。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS 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に、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載の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。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。あるいは、次のフォームを使用して、シスコ セキュリティ アドバイザリに該当するリリースであるかどうかを確認します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. リリース番号（例：15.9(3)M2、17.3.3）を入力します。
3. [チェック（Check）] をクリックします。

2 | | Critical,High,Medium

このアドバイザのみ

Enter release number | Check

不正利用事例と公式発表

Cisco PSIRT では、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は確認しておりません。

出典

この脆弱性は、シスコ内部でのセキュリティテストの際に、シスコのMichael Deviceによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-dos-95Fqnf7b

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	2025年5月7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。