Cisco IOSおよびIOS XEソフトウェアのFXOインターフェイスにおける宛先パターンバイパスの脆弱性

アドバイザリーID : cisco-sa-fxo-pattern-bypass-jUXgygYv
初公開日 : 2021-09-22 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 : CSCvw53542

CVE-2021-34705

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Voice Telephony Service Provider(VTSP)サービスの脆弱性により、認証されていないリモートの攻撃者が設定された宛先パターンをバイパスし、任意の番号をダイヤルできる可能性があります。

この脆弱性は、Foreign Exchange Office(FXO)インターフェイスでのダイヤル文字列の検証が不十分であることに起因します。攻撃者は、ISDNプロトコルまたはSIPのいずれかを介して該当デバイスに不正なダイヤル文字列を送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は通話料金の不正を行い、影響を受けるお客様に予期しない財務上の影響を与える可能性があります。

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-fxo-pattern-bypass-jUXgygYv

このアドバイザリは、Cisco IOS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公開の2021年9月リリースの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: September 2021 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

この脆弱性は、Cisco IOSまたは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ているシスコデバイスに影響を与えます。次の両方に該当します。

- FXOインターフェイスに少なくとも1つのワイルドカードが設定された宛先パターンがあります。
- デバイスは、ISDNまたはSIPを介した着信コールをサポートするように有効化されています。

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。

FXOインターフェイス設定の確認

FXOインターフェイスの設定を確認するには、まずshow inventory | | include FXOコマンドをデバイスのCLIで実行して、少なくとも1つのFXOインターフェイスカードがデバイスにインストールされているかどうかを確認します。このコマンドで空の出力が返された場合は、FXOインターフェイスカードがインストールされておらず、デバイスに脆弱性はありません。

次に、show inventory | include FXOコマンドを、サブスロット0/3にFXOインターフェイスカードが取り付けられているデバイスで実行した場合の出力例を示します。

<#root>

ios#

show inventory | include FXO

NAME: "NIM

subslot 0/3

", DESCR: "NIM-4FXO Voice Analog Module"
PID: NIM-4

FXO

          , VID: V02 , SN: XXXXXXXXXXX

上記のコマンドで出力が返される場合は、コマンド出力の（サブ）スロット番号をメモします。

次に、show running-config | section dial-peer voiceコマンドを使用して、次の条件をすべて満たす出力セクションを探します。

- 出力は、dial-peer voice tag potsで始まります。
- エントリにdestination-pattern patternが含まれており、patternには少なくとも1つのワイルドカード文字が含まれています。
- 同じエントリがport x/y/zを示しています。ここで、x/y/zは、前述のshow inventoryからの出力に関連するFXOインターフェイスカード上のポートです | | include FXOコマンドを使用します。

次の例は、show running-config | セクションdial-peer voiceの出力では、エントリの宛先パターンにドット(.)ワイルドカード文字が含まれ、タグ35のダイヤルピアがサブスロット0/3のFXOインターフェイスカードにリンクされています。

```
<#root>

ios#

show running-config | section dial-peer voice


.
.
.

dial-peer voice

 35

pots



destination-pattern

 123

.



port 0/3

/5
 forward-digits all
.
.
.
```

ISDNインターフェイス設定の確認

デバイスに ISDN インターフェイスが設定されているかどうかを判断するには、CLI で show running config | include isdn switch-type コマンドを使用します。 | include isdn switch-type コマンドにより識別できます。値が返る場合、ISDN インターフェイスが有効になっています。

次の例は、ISDNインターフェイスを持つデバイスでのコマンドの出力を示しています。

```
<#root>

ios#

show running-config | include isdn switch-type



isdn switch-type

 primary-net5
```

注：正確なスイッチタイプは、この脆弱性には影響しません。

SIP設定の決定

show running-configまたはshow running-config allの出力に表示されないデフォルトのdial-peer voice tag voipでは、着信SIPコールがサポートされています。したがって、特定の設定は必要ありません。

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。

- 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。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 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

この脆弱性を報告していただいた Austin Martinetti 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxo-pattern-bypass-jUXgygYv

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	2021 年 9 月 22 日

利用規約

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。