Catalyst 9000 ファミリ向け Cisco IOS XE ワイヤレス コントローラ ソフトウェアの CAPWAP モビリティ処理におけるサービス妨害（DoS）の脆弱性

アドバイザリーID : cisco-sa-c9800-mob-dos-342YAc6J
初公開日 : 2022-09-28 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 : CSCwa92678

CVE-2022-20856

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

Catalyst 9000 ファミリ向け Cisco IOS XE ワイヤレスコントローラ ソフトウェアにおける Control and Provisioning of Wireless Access Points（CAPWAP）モビリティメッセージ処理の脆弱性により、認証されていないリモートの攻撃者が、該当デバイスでサービス妨害（DoS）状態を引き起こす可能性があります。

この脆弱性は、CAPWAP モビリティメッセージの処理に関連する論理エラーとリソースの不適切な管理に起因します。攻撃者は、細工を施した CAPWAP モビリティパケットを該当デバイスに送信することで、この脆弱性をエクスプロイトできる可能性があります。エクスプロイトに成功すると、該当デバイスでリソースを枯渇させることが可能になります。これによりデバイスのリロードが引き起こされ、その結果 DoS 状態に陥る危険性があります。

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-c9800-mob-dos-342YAc6J

このアドバイザリは、2021 年 9 月に公開された Cisco IOS および IOS XE ソフトウェア セキュリティ アドバイザリバンドルの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: September 2022 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

脆弱性のある Cisco IOS XE ソフトウェアリリースを実行し、モビリティグループに属する（デフォルトでは無効）次のシスコ製品が、この脆弱性の影響を受けます。

- クラウド向け Catalyst 9800-CL ワイヤレスコントローラ
- Catalyst 9300、9400、9500 シリーズ スイッチ用 Catalyst 9800 組み込みワイヤレスコントローラ
- Catalyst 9800 シリーズ ワイヤレス コントローラ

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。

デバイス設定の確認

デバイスがモビリティグループに属する場合、この脆弱性の影響を受けます。デバイスがモビリティグループに属しているかどうかを確認するには、コマンド show wirelessmobility summary を使用します。このコマンドによって生成された出力結果の最後に、現在のコントローラを含むモビリティピアが、モビリティドメインで設定されたコントローラの下に一覧表示されます。現行デバイスのみが表示されている場合、デバイスはモビリティグループには属しておらず、脆弱性の影響を受けません。現行デバイス以外のデバイスが表示されている場合、そのデバイスはモビリティグループに属しており、脆弱性の影響を受けます。

以下の出力例（分かりやすくするためにレイアウトを変更）は、コマンドが発行されたデバイスとそのモビリティピアの 2 つのデバイスを示しています。したがって、例のデバイスはモビリティグループに属しており、脆弱性の影響を受けます。

<#root>

```
WLC#show wireless mobility summary
Mobility Summary


Wireless Management VLAN: 999
Wireless Management IP Address: 9.9.9.9
Wireless Management IPv6 Address:
Mobility Control Message DSCP Value: 48
Mobility High Cipher : False
Mobility DTLS Supported Ciphers: TLS_ECDHE_RSA_AES128_GCM_SHA256, TLS_RSA_AES256_GCM_SHA384, TLS_RSA_
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: default
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: 001e.ffff.ffff
```

```
Mobility Domain Identifier: 0x34ac
```

Controllers configured in the Mobility Domain:

IP	パブリック IP	MAC アドレス	グループ名	マルチキャスト IPv4	マルチキャスト IPv6	ステータス	PMTU
9.9.9.9	N/A	001e.ffff.ffff	デフォルト	0.0.0.0	::	N/A	N/A
9.9.9.10	9.9.9.10	001e.ffff.fffe	デフォルト	0.0.0.0	::	2013 年以降	1385

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。

- Catalyst アクセスポイントの組み込みワイヤレスコントローラ
- 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
- ワイヤレス LAN コントローラ（WLC）AireOS ソフトウェア

セキュリティ侵害の痕跡

『Cisco Security Indicators of Compromise Reference Guide』にはよく見られる IoC が記載されており、このシスコ セキュリティ アドバイザリで公開されている脆弱性の影響を受ける可能性のあるデバイスを特定するのに役立ちます。

この脆弱性がエクスプロイトされると、該当デバイスで mobilityd プロセスがクラッシュする可能性があります。デバイスで mobilityd のクラッシュが発生すると、クラッシュログバンドルに次のメッセージが表示されることがあります。

```
Feb 15 19:15:43.331: %ID_MANAGER-3-INVALID_ID: Chassis 1 R0/0: mobilityd: bad id in id_get (Out of IDs!)
```

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

お客様が 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（15.9(3)M2、17.3.3 など）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 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-c9800-mob-dos-342YAc6J

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 9 月 28 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。