

Catalyst 9800シリーズWireless Controller用 Cisco IOS XEソフトウェアのCloud Unauthenticated Access to Certificate Enrollment Serviceの脆弱性



アドバイザリーID : cisco-sa-9800cl-

openscep-SB4xtxzP

初公開日 : 2025-09-24 16:00

バージョン 1.0 : Final

CVSSスコア : [5.3](#)

回避策 : Yes

Cisco バグ ID : [CSCwh91048](#)

[CVE-2025-20293](#)

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for Catalyst 9800 Series Wireless Controllers for Cloud(9800-CL)のDay Oneセットアッププロセス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、該当デバイスで実行されている公開キーインフラストラクチャ(PKI)サーバにアクセスできる可能性があります。

この脆弱性は、Day Oneセットアッププロセスの完了時にクリーンアップが不完全であることに起因します。攻撃者は、Simple Certificate Enrollment Protocol(SCEP)要求を該当デバイスに送信することにより、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、仮想ワイヤレスコントローラから証明書を要求し、取得した証明書を使用して、攻撃者によって制御されるデバイスを仮想ワイヤレスコントローラに参加させることができます。

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。本脆弱性に対処する回避策がいくつかあります。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-9800cl-openscep-SB4xtxzP>

このアドバイザリーは、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ーバンドル公開の2025年9月リリースの一部です。これらのアドバイザリー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 \(半年刊、2025年9月 \)](#)』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、デバイス設定に関係なく、この脆弱性はCatalyst 9800シリーズWireless Controller for CloudのCisco IOS XEソフトウェアに影響を与えました。

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。

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。

シスコは、この脆弱性がCatalyst 9800シリーズワイヤレスハードウェアベースコントローラのCisco IOS XEソフトウェアには影響を与えないことを確認しました。

回避策

この脆弱性に対処する回避策はありません。管理者は、ワイヤレスLANコントローラ(WLC)のホスト名と一致するホスト名を持つhostname_WLC_CA PKIサーバをシャットダウンできます。次の出力は、WLCホスト名がvewlcの例で実行する必要がある手順を示しています。

```
<#root>
```

```
vewlc# conf t  
vewlc(config)# crypto pki server
```

```
vewlc_WLC_CA
```

```
vewlc(cs-server)# shutdown  
vewlc(cs-server)# exit  
vewlc# write memory
```

この回避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

シスコでは、修正済みソフトウェアリリースへのアップグレードが利用可能になるまで、回避策や緩和策は一時的な解決策であると考えています。この脆弱性を完全に修復し、本アドバイザリで説明されている障害の発生を回避するために、お客様には本アドバイザリで説明されている修正済みソフトウェアにアップグレードすることを強く推奨します。

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 Product Security Incident Response Team (PSIRT) では、本アドバイザリに記載されている脆弱性のエクスプロイト事例とその公表は確認しておりません。

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-9800cl-openscep-SB4xtxzP>

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9月24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、単独の転載や意識を施した場合、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。