# Cisco IOS XE ワイヤレス コントローラ ソフトウェアにおける任意のファイルアップロードの脆弱性


アドバイザリーID : cisco-sa-wlc-file-uplpd-rHZG9UfC
CVE-2025-20188
初公開日 : 2025-05-07 16:00
最終更新日 : 2025-06-06 20:02
バージョン 2.2 : Final
CVSSスコア : 10.0
回避策 : Yes
Cisco バグ ID : CSCwk33139

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

Wireless LAN Controller(WLC)向けCisco IOS XEソフトウェアのアウトオブバンドアクセスポイント(AP)イメージダウンロード、Clean Airスペクトル記録、およびクライアントデバッグバンドル機能の脆弱性により、認証されていないリモートの攻撃者が該当システムに任意のファイルをアップロードする可能性があります。

この脆弱性は、ハードコードされた JSON Web トークン（JWT）が該当システムに存在することに起因します。 攻撃者は、巧妙に細工されたHTTPS要求をAPファイルアップロードインターフェイスに送信することで、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 root 権限を使用して、ファイルのアップロード、パストラバーサルの実行、および任意のコマンドを実行でき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。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-wlc-file-uplpd-rHZG9UfC

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。アドバイザリとリンクの一覧については、『Cisco Event Response: May 2025 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、デバイスの設定に関係なく、WLC 用の 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ている以下のシスコ製品に影響を与えます。

- 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
- Catalyst AP の組み込み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。

## 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 ソフトウェア
- WLC として機能しておらず、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ないデバイスで実行されている IOS XE 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
- WLC AireOS ソフトウェア

# 回避策

考えられる 2 つのデバイス設定について、この脆弱性に対処するために推奨される 2 つの軽減策があります。

影響を受ける機能が使用されていない

影響を受ける機能が使用されていない場合は、次の例に示すように、インフラストラクチャ アクセス コントロール リスト（iACL）をすべてのインターフェイスに適用し、インターフェイスを完全にブロックします。これにより、脆弱性が完全に軽減されます。

```
wlc# show ap file-transfer https summary
Configured port : 8443
Operational port : 8443

wlc# show ip access-lists CVE-2025-20188
  10 deny tcp any any eq 8443
  20 permit ip any any
```

### 影響を受ける機能が使用されている

影響を受ける機能が使用されている場合は、攻撃対象領域を減らすために、iACL を適用して WLC への AP ファイル アップロード インターフェイスを制限し、想定される送信元からのトラフィックのみを許可します。次に、展開された iACL の一部として含めることができる iACL の例を示します。

```
wlc# show ap file-transfer https summary
Configured port : 8443
Operational port : 8443

wlc# show ip access-lists CVE-2025-20188
  10 deny tcp any INFRASTRUCTURE_ADDRESSES WILDCARD eq 8443
  20 permit ip any any
```

iACL の展開手法のガイドラインと推奨事項については、ホワイトペーパー『コアの保護：インフラストラクチャ保護 ACL』を参照してください。

また、この脆弱性に対処する回避策があります。

次の例に示すように、AP クライアント デバッグ バンドルを手動で 1 回トリガーすると、AP ファイル アップロード インターフェイスを使用する、影響を受けるすべての機能が保護されます。この回避策はリロード後も維持されることはないため、デバイスをリロードするたびに実行する必要があることに注意してください。

```
! Check and pick any one client in any AP associated with this WLC
wlc# show wireless client summary
Number of Clients: 1

MAC Address       AP Name                Type ID   State   Protocol   Method   Role
-------------------------------------------------------------------------------------
5eef.1000.0001    AP5EEF.1000.0003       WLAN 1    Run     11n(5)     None     Local

Number of Excluded Clients: 0

! Manually trigger the debug bundle once
wlc# debug wireless bundle client mac 0100.5eef.1000.0001
Wireless Client debug bundle add event
```

```
! Get the site-tag
wlc# show ap tag summary | inc AP5EEF.1000.0003|AP Name



AP Name           AP Mac          Site Tag Name Policy Tag Name  RF Tag Name  Misconfigured Tag Source
AP5EEF.1000.0003  5eef.1000.0003  ST1           policy-tag        rf-tag       No            Static



! Be sure to change the monitor-time to 60 so this process will take 60 seconds and not longer
wlc# debug wireless bundle client start ap-archive site-tag ST1 level debug monitor-time 60

! Stop debug bundle after 60 seconds
wlc# debug wireless bundle client stop-all collect all

! A debug bundle should be generated and the workaround was successfully executed
wlc# dir bootflash:completeCDB/*
2883591   -rw-      383488    Jan 6 2025 11:18:25 +00:00    wireless_bundle_0100.5eef.1000.0001.tar
96739794944 bytes total (75825774592 bytes free)
```

これらの回避策と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

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 シスコサポート & ダウンロードページには、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。

## 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 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 は、このアドバイザリで説明されている脆弱性に対してコンセプト実証エクスプロイトコードが利用可能であることを認識しています。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

## 出典

この脆弱性は、内部セキュリティテストの実施中に、Cisco Advanced Security Initiatives Group（ASIG）の X.B. によって発見されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | 日付 |
|---|---|---|---|---|
| 2.2 | 軽減策を更新。 | 回避策 | Final | 2025 年 6 月 6 日 |
| 2.1 | 推奨方法として、回避策よりも軽減策を優先。 | 回避策 | Final | 2025 年 6 月 6 日 |
| 2.0 | 影響を受ける 2 つの機能を追加。脆弱性の設定条件を更新。回避策と軽減策を追加。シスコがコンセプト実証コードを認識しているという事実を追加。 | サマリー、脆弱性のある製品、回避策、エクスプロイト事例および公式発表 | Final | 2025 年 6 月 6 日 |
| 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。