

IOS-XEセキュリティアドバイザリ – 2026年8月 および関連する重大な問題の修正

内容

はじめに

このドキュメントでは、IOS-XEアドバイザリ (2026年8月) 用に公開された強化されたセキュリティリリースに関して報告された重要なワイヤレスソフトウェアの不具合について説明します。

背景

このドキュメントでは、[セキュリティアドバイザリ](#)、[FN74383](#)、および重大な問題に対処するためのアップグレードガイダンスを提供します。

2026年8月5日、シスコは9800シリーズWireless LAN Controllerを含む複数のプラットフォームに影響を与える[IOS-XE Security Hardening Advisory](#)をリリースしました。文書化されているように、このアドバイザリは、Cisco IOS-XEエンジニアリングによる包括的な内部セキュリティレビューの結果として内部で発見された複数の脆弱性に対処します。

レビューに含まれるワイヤレスプラットフォーム

Catalyst Wireless 9800(C9800-L、C9800-CL、C9800-40、C9800-80)

Cisco Wireless 9800 WLC(CW9800L、CW9800M、CW9800H1/H2)

Catalystスイッチ(9800-SW)上の組み込みワイヤレス9800:SDA展開のみをサポート

COS ベースの Catalyst 11ax 91xx シリーズ アクセスポイント
(9105/9115/9117/9120/9130/9136/9164/9166)

Cisco Wireless 917xシリーズアクセスポイント
(CW9171/CW9172/CW9174/CW9176/CW9178/CW9179)

Cisco IOS XE ソフトウェア リリース	First Fixed Release (修正された最初のリリース)
--------------------------	--------------------------------------

17.9	17.9.10
17.12	17.12.8
17.15	17.15.6
17.18	17.18.4、17.18.4a*
26.1	26.1.2

表 1.レビューに含まれるソフトウェアリリースと対応する強化リリース

 *注:17.18.4aでは、すべてのスタンドアロンWLCがサポートされます。17.18.4スイッチリリースで動作する17.18.4ワイヤレスパッケージを使用するのは、SDA展開でスイッチに組み込まれているワイヤレスLANコントローラ(WLC)だけです。スイッチまたはワイヤレスパッケージ用の17.18.4aバージョンはありません。

重要なバグ

表1に示すセキュリティ強化されたリリースでは、これらのリリースの使用に影響を与える可能性のある重大な問題がいくつか特定されています。

- 1. [CSCwv93265](#)
- 2. [CSCwv98483](#)

重要なバグの詳細

[CSCwv93265](#)

症状：OpenRoaming、WPA3、11k、11v、11r機能が使用中の場合のクライアント接続またはローミングの失敗。
該当するプラットフォーム：すべてのCisco 9800ワイヤレスコントローラおよびCat9K用ワイヤレスパッケージ。
該当するソフトウェアバージョン：Cisco IOS XE 26.1.2、Cisco IOS XE 17.18.4a、Cisco IOS XE 17.18.4、Cisco IOS XE 17.15.6、Cisco IOS XE 17.12.8、Cisco IOS XE 17.9.10
次のステップ：17.12.8、17.15.6、および17.18.4aに対して修正済みAPSPが利用可能です。その他のIOS XEバージョン(17.9.10、26.1.2)の修正APSPは、8月15日までにリリースされる予定です。APSPのリリース後は、APSPを導入することをお勧めします。
修正済みリリース:

	C9800-L	CW9800-L	C9800-40	C9800-80	C9800-CL	CW9800-M	CW9800-H1	CW9800-H2	cat9kスイッチ	C9350	EWC-on-9100s
17.15.6	APSPリンク	NA	APSPリンク	APSPリンク	APSPリンク	APSPリンク	APSPリンク	APSPリンク	APSPリンク	NA	TACに連絡して Engineering Specialビル

											ドを取得
17.18.4a	APSPリンク	APSPリンク	APSPリンク	APSPリンク	APSPリンク	APSPリンク	APSPリンク	APSPリンク	NA	NA	NA
17.18.4	NA	NA	NA	NA	NA	NA	NA	NA	APSPリンク	NA	NA
17.12.8	APSPリンク	NA	APSPリンク	APSPリンク	APSPリンク	NA	NA	NA	APSPリンク	NA	17.15トレインに移行
26.1.2	8月15日に予定	8月15日に予定	8月15日に予定	8月15日に予定	8月15日に予定	8月15日に予定	8月15日に予定	8月15日に予定	8月15日に予定	8月15日に予定	NA
17.9.10	APSPリンク	NA	APSPリンク	APSPリンク	APSPリンク	NA	NA	NA	APSPリンク	NA	17.15トレインに移行

表 2 異なる9800 WLCプラットフォーム用のAPSPリンク

[CSCwv98483](#)

症状：C9800-L、CW9800-L、C9800-CLが外部WLCとして設定されている場合、アンカーされたワイヤレスクライアントがIP_Learnでスタックする

該当するプラットフォーム：C9800-L、CW9800-L、C9800-CL (該当するプラットフォームが外部WLCとして機能するゲスト/アンカーシナリオのみ)

該当するソフトウェアバージョン：Cisco IOS XE 26.1.2、Cisco IOS XE 17.18.4a、Cisco IOS XE 17.15.6

回避策：外部とアンカーの間のトンネルでモビリティデータリンク暗号化を有効にします。

wireless mobility group member mac-address

ip

public-ip

group

data-link-encryption

通知されます (リリース予定 : 8月21日)。これは、WLCのリロードを必要とするコールドSMUになります。

アドバイザリおよび重大な問題に関するアップグレードガイド ス

セキュリティ強化されたリリースに関して報告されるアドバイザリ問題と重大な問題の両方に対処するために、シスコは次の項目を推奨します

ステップ 1 : IOS-XEバージョン17.12、17.15、17.18を実行しているワイヤレス環境のお客様は、ステップ2、3、および4に進みます。IOS-XEバージョン17.9および26.1を実行しているワイヤレス環境のお客様は、APSPパッチが cisco.comに公開されるのを待ってからアップグレードしてください。パッチのリリース日については、表2を参照してください

ステップ 2アップグレードの前に、[ここに](#)に記載されているアップグレードチェックと回復の手順を実行して、[FN74383](#)

ステップ 3セキュリティが強化されたIOS-XEバージョンとAPSPパッチを同じメンテナンス時間帯にアップグレードして、ワイヤレスサービスへの影響を回避します。

ステップ 4CSCwv98483の影響を受ける場合、SMUが使用可能になるまで回避策を適用します。SMUがポストされると、お客様はSMUパッチを適用する必要があります。

IOS-XEアップグレード+パッチのメンテナンス時間帯を計画する 際のダウンタイムに関する考慮事項

非冗長または高可用性(HA)冗長構成で構成された9800 WLCでのIOS-XEアップグレードでは、次のようなさまざまなメカニズムを利用できます

- In-Service Software Upgrade (ISSU)
- N+1ローリングアップグレード
- ワンショットアップグレード

詳細については、『[9800 WLCアップグレードクイックスタートガイド](#)』を参照してください。

さらに、重大な問題には、ソフトウェアメンテナンスアップデート(SMU)とアクセスポイントのサービスパック(APSP)によるパッチ適用が必要です

9800 WLCでサポートされる各種パッチングオプションの詳細については、『[9800 WLC用のパッ](#)

[パッチ適用およびローリングAPアップグレードガイド](#)』を参照してください。

各アップグレードメカニズムでIOS-XEアップグレード+パッチ適用のメンテナンス期間を計画するには、このセクションで説明するダウンタイムと影響を考慮します。

In-Service Software Upgrade (ISSU)

- HA Stateful Switchover(HA SSO)設定で実行されている9800 WLCペアだけに適用され、長期間使用されるリリーストレインとそれらのメンテナンスリリースの間でのみサポートされます。(メンテナンスリリースのないエスカレーションリリースおよび短期リリーストレインではサポートされません)
- ISSUは、異なるソフトウェアバージョンを実行し、ローリングAPアップグレードを活用しながら、HA SSOで9800ペアをサポートすることにより、シームレスなアップグレードエクスペリエンスを提供します。稼働中の9800 HAペアでは、スタンバイWLCがアップグレードされ、SSO後には新しいスタンバイWLCがアップグレードされます。ISSUプロセスと、対応するCLIおよびGUIスナップショットの詳細については、「[ISSUを使用した9800 HA SSOのアップグレード](#)」を参照してください。
- ISSUを開始する前に、APでアップグレードチェックと回復を実行します。
- ISSUでは、アップグレード期間を簡単に予測できません。導入規模やネットワーク速度によっては、アップグレードの完了に数時間かかる場合があります
- さらに、ISSUではローリングAPアップグレードを活用し、段階的にAPをリブートすることでダウンタイムを最小限に抑えています。ただし、この場合、強化されたリリースを実行しているAPに接続しているクライアントでは、ISSUアップグレード後にWLCにパッチが適用されるまで、[CSCwv93265](#)および[CSCwv98483](#)に記載されている接続とローミングの問題が発生し続けることを意味します。
- [CSCwv98483](#)のSMUは、WLCのリロードを必要とするコールドパッチです。
- [CSCwv93265](#)のAPSPは、ローリングAPアップグレードを使用して、またはワンショットで適用できます。展開規模によっては、ローリングAPアップグレードを使用する場合、すべてのAPをアップグレードするのに数時間かかる可能性があり、既知の重大な不具合を確実に回避できます
- サービスに影響する可能性がある合計期間 (WLCまたはAPがダウンしているか、クライアント接続/ローミングが影響を受けている) = ISSUの完了までの時間+ SMUコールドパッチによるWLCのリロードまでの時間+ APSPのAPローリングアップグレードまでの時間

N+1ローリングAPアップグレード

- この手順は、「実稼働」の9800ペアまたは9800スタンドアロンがアップグレードされている間に、N+1 WLCと呼ばれるスペアの9800 WLCを使用してソフトウェアバージョンをホストAPにアップグレードすることに依存しています。N+1ローリングアップグレードを開始する前に、このN+1 9800 WLCにAPを登録しないことをお勧めします。
- プライマリWLCに登録されているAPで、アップグレードチェックと回復を実行します
- プロセスと、関連するCLIおよびGUIスナップショットの詳細については、『[N+1ローリングAPアップグレードを使用した9800 WLCのアップグレード](#)』を参照してください。
- このプロセスでは、APがプライマリWLCからN+1 WLCにシームレスにロールオーバーする

ためには、N+1 WLCで実行され、APに事前にダウンロードされたソフトウェアバージョンが正確に一致している必要があります。

- APへのプレダウンロードは、プライマリWLCでIOS-XE強化リリースをダウンロードし、アクティブ化しないことによって容易になります。イメージをアクティブ化しないと、ソフトウェアパッチをAPに適用したり、事前にダウンロードしたりすることはできません。これは、N+1 WLCにもパッチを適用できないことを意味します。
- ISSUのようにこのプロセスでも、N+1 WLCにロールオーバーされたAPは、N+1 WLCにパッチが適用されるまでは、Rolling APのアップグレードが完了した後も、[CSCwv93265](#)および[CSCwv98483](#)に記載されているクライアント接続およびローミングの問題が発生する危険性があります。
- [CSCwv98483](#)のSMUは、WLCのリロードを必要とするコールドパッチです。
- [CSCwv93265](#)のAPSPは、ローリングAPアップグレードを使用して、またはワンショットで適用できます。展開規模によっては、ローリングAPアップグレードを使用する場合、すべてのAPをアップグレードするのに数時間かかる可能性があり、既知の重大な不具合を確実に回避できます
- サービスに影響する可能性のある合計期間 (WLCまたはAPのいずれかがダウンしているか、クライアント接続/ローミングが影響を受けている) =すべてのAPがN+1のWLCにロールオーバーするのに要した時間+ SMUコールドパッチが原因でWLCがリロードされるまでの時間+ APSPのAPローリングアップグレードまでの時間
- メンテナンス時間帯には、N+1 WLCをIOS-XE強化リリースにアップグレードするために要した時間、およびAPがプライマリWLCからIOS-XE強化リリースをプレダウンロードするために要した時間も考慮しますが、これらのいずれもサービスに影響しません

N+1通常のAPアップグレード：推奨

- この手順は、「実稼働」の9800ペアまたは9800スタンドアロンがアップグレードされる間にソフトウェアバージョンがホストAPにアップグレードされたN+1 WLCとしてスペアの9800 WLCコールに依存します。
- N+1ローリングアップグレードを開始する前に、このスペア9800 WLCにAPを登録しないことをお勧めします。
- スペアのN+1 WLCは、強化されたIOS-XEのアクティブ化およびコミットにアップグレードでき、APSPおよびSMUでパッチを適用できます。APが登録されていない場合、これはサービスに影響しませんが、メンテナンス時間帯をスケジュールする際には、複数のWLCのリロードにかかる時間を考慮する必要があります
- APが登録されているプライマリWLC GUIで、Configuration > Tags and Profiles: AP Priming > Primary Baseの順に移動します
 - N+1 WLCとワイヤレス管理インターフェイス(WMI)のIPアドレスをプライマリとして定義する
 - セカンダリで現在のプライマリWLC名とWMI IPを定義します。
- 正規表現フィルタを使用して、APをプライマリWLCからN+1 WLCに一括移行します。
- N+1 WLCに登録すると、APではすでにセキュリティ強化リリースと、重大な不具合を修正するパッチが実行されています。

サービスに影響する可能性のある合計期間 (WLCまたはAPのどちらかがダウンしているか、クライアント接続/ローミングが影響を受ける) = APがプライマリWLCからN+1 WLCに移行するのにかかる時間。これは、APとWLC間のネットワーク速度によって決定されます。

ワンショットアップグレード：N+1 WLCが存在しない場合に推奨

- この手順では、プライマリWLCを（アクティブ化およびコミットメントとともに）セキュリティ強化されたIOS-XEリリースに1ステップでアップグレードします。
- イメージアクティベーションの一部として、プライマリWLCがリロードされ、すべてのAPがアップグレードプライマリWLCに再登録され、セキュリティが強化されたIOS-XEリリースを受け取ります。
- APSPが適用されるまでは、[CSCwv93265](#)および[CSCwv98483](#)に記載されているクライアント接続とローミングの問題によってAPにリスクが生じます

サービスに影響する可能性がある（WLCまたはAPがダウン、またはクライアント接続/ローミングが影響を受ける）合計期間=プライマリWLCのリロードにかかった時間+すべてのAPがCAPWAPを介してプライマリWLCから強化されたIOS-XEリリースをダウンロードし、プライマリWLCに再登録にかかった時間（SMUパッチが適用されている場合は2倍）+すべてのAPがプライマリWLCからAPSPパッチをを取得し、プライマリしてWLC再登録してWLCに再登録戻してかかった時間

FAQ

Q1.APはこのセキュリティアドバイザリの影響を受けますか。

セキュリティレビューにはCOSベースのアクセスポイントが含まれており、対応する修正が強化されたIOS-XEリリースに組み込まれています

Q2.AireOS WLCのリスクは何ですか。

AireOS WLCはサポート終了日(LDoS)に達したため、セキュリティレビューに含まれませんでした

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。