Cisco IOS アクセス ポイント ソフトウェア 802.11r Fast Transition におけるサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20181017-ap-ft-dos

初公開日 : 2018-10-17 16:00

バージョン 1.0 : Final

CVSSスコア : 7.4

回避策 : No workarounds available

Cisco バグ ID : CSCve64652

CVE-2018-0441

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 のアクセス ポイント（AP）ソフトウェア、802.11r Fast Transition の機能セットに存在する脆弱性により、近接する未認証の攻撃者が、該当のデバイスにサービス妨害（DoS）の状態を引き起こす可能性があります。

この脆弱性は、特定のローミング イベントが原因で特定のタイマー メカニズムが機能しなくなることにより発生し、 この不具合によってタイマーがクラッシュします。 攻撃者は、この脆弱性を不正利用して、同じ AP に対し、悪意のある再アソシエーションのイベントを短時間に複数回送信することで、該当の AP に DoS 状態を引き起こします。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181017-ap-ft-dos

該当製品

脆弱性のある製品

Cisco IOS アクセス ポイント ソフトウェアの該当バージョンが実行されている Cisco アクセス ポイントが、この脆弱性の影響を受けます。

脆弱性が存在する Cisco アクセス ポイント 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」の項を参照してください。

Cisco アクセス ポイント ソフトウェア リリースの判別

デバイス上で実行されている Cisco アクセス ポイント ソフトウェアのリリースは、管理者が、コントローラの Web インターフェイスまたは CLI を使用して確認できます。

コントローラの Web インターフェイスを使用する場合は、次を実行します。

1. コントローラの Web インターフェイスにログインします。
2. [モニタ（Monitor）] タブをクリックします。
3. 左側のペインで [概要（Summary）] をクリックします。
4. [コントローラの概要（Controller Summary）] の [ソフトウェア バージョン（Software Version）] フィールドは、デバイスで現在実行されているソフトウェアのリリース番号を示します。

アクセス ポイントの CLI を使用するには、Telnet セッションでアクセス ポイントにログインします。 show version | | include IOS コマンドを発行し、その出力結果を参照してください。次の例は、Cisco IOS ソフトウェア リリース 15.3(3)JA12 を実行中の Cisco アクセス ポイントの出力結果を示します。

```
AP# show version | include IOS

Cisco IOS Software, C1600 Software (AP1G2-K9W8-M),

Version 15.3(3)JA12, RELEASE SOFTWARE (fc2)

AP#
```

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が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

AP-COS ソフトウェアを実行中の Cisco アクセス ポイントは、この脆弱性の影響を受けません。

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 アップデートを提供しています。 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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、Cisco Security Advisories and Alerts 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 に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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。

修正済みリリース

シスコはこの脆弱性に対処する修正済みソフトウェアをリリースしました。

本アドバイザリは以下のアドバイザリを含むコレクションの一部です。これらも考慮した上、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。

- cisco-sa-20181017-wlc-gui-privesc: シスコ ワイヤレス LAN コントローラ ソフトウェア GUI の特権昇格の脆弱性

- cisco-sa-20181017-ap-ft-dos: Cisco IOS アクセス ポイント ソフトウェア 802.11r Fast Transition におけるサービス妨害（DoS）の脆弱性
- cisco-sa-20181017-wlc-capwap-memory-leak: シスコ ワイヤレス LAN コントローラ ソフトウェア Control and Provisioning of Wireless Access Points プロトコルにおける情報漏えいの脆弱性
- cisco-sa-20181017-wlc-capwap-dos: シスコ ワイヤレス LAN コントローラ ソフトウェア Control and Provisioning of Wireless Access Points プロトコルにおけるサービス妨害の脆弱性

カスタマーは、このセクションの表に沿って、適切なリリースへのアップグレードをおこなってください。 次の表で、最初の列は、シスコ ワイヤレス LAN コントローラ ソフトウェアのメジャー リリース、2 列目と 3 列目はそれぞれ、このアドバイザリで述べた脆弱性に対処する、シスコ ワイヤレス LAN コントローラ ソフトウェアの最初の修正済みリリース、および対応する Cisco AP IOS ソフトウェアの最初の修正済みリリースを示します。

Cisco WLC メジャー ソフトウェア リリース	この脆弱性に対する最初の Cisco WLC 修正済みリリース	この脆弱性に対する最初の Cisco AP IOS 修正済みリリース
Prior to 8.0	脆弱性あり、8.3.140.0 以降に更新	脆弱性あり、15.3(3)JD13 以降に更新
8.1	脆弱性あり、8.3.140.0 以降に更新	脆弱性あり、15.3(3)JD13 以降に更新
8.2	脆弱性あり、8.3.140.0 以降に更新	脆弱性あり、15.3(3)JD13 以降に更新
8.3	脆弱性あり、8.3.140.0 以降に更新	脆弱性あり、15.3(3)JD13 以降に更新
8.4	脆弱性あり、8.5.110.0 以降に更新	脆弱性あり、15.3(3)JF4 以降に更新
8.5	脆弱性あり、8.5.110.0 以降に更新	脆弱性あり、15.3(3)JF4 以降に更新
8.6	脆弱性なし	脆弱性なし
8.7	脆弱性なし	脆弱性なし
8.8	脆弱性なし	脆弱性なし

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やその公表を確認していません。

出典

この脆弱性は、Cisco TAC のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181017-ap-ft-dos

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-October-17

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。