Cisco IOS アクセス ポイント ソフトウェア 802.11r Fast Transition における Denial of Service（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20190717-aironet-dos

初公開日 : 2019-07-17 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 : CSCvg95745

CVE-2019-1920

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 アクセス ポイント（AP）ソフトウェアの 802.11r Fast Transition（FT）の実装における脆弱性により、認証されていない近接する攻撃者が、該当のインターフェイスにサービス妨害（DoS）状態を引き起こす可能性があります。

この脆弱性は、FT 用に設定されたターゲット インターフェイスに送信されるクライアント認証要求に対する完全なエラー処理条件が欠如していることに起因します。 攻撃者が、巧妙に細工された認証要求トラフィックをターゲット インターフェイスに送信することによって、この脆弱性をエクスプロイトし、その結果デバイスが予期せず再起動する恐れがあります。

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ました。 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-20190717-aironet-dos

該当製品

脆弱性のある製品

802.11r 用に設定された 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。

CLI からの 802.11r Fast Transition（FT）設定の確認：

手順：

AP が関連付けられている WLC の CLI から、デバイスに 802.11r FT 機能が設定されているかどうかを確認するために、管理者は、次の **show** コマンドを発行することができます。

コマンド：

(Cisco Controller) > **show wlan <*wlan id*>**

(Cisco Controller) > **show wlan <*wlan id*>**

Security

Security

FT Support.....Disabled

FT Support.....Disabled

FT Support.....Disabled

FT Support.....Disabled

（GUI）からの 802.11r Fast Transition（FT）設定の確認：

手順：

ステップ 1： [**WLANs**] タブを選択して、[WLANs] ウィンドウを開きます。
ステップ 2： [**WLAN ID**] をクリックします。
ステップ **3：** [Security] > [**Layer 2**] を選択して、Fast Transition 機能がデバイスで有効になっているか、または無効になっているかを確認します。

各 WLAN の 802.11r Fast Transition を設定するときに、ドロップダウン メニュー内に存在する使用可能な**適応型**オプションに注意することが重要です。 この機能を選択すると、互換性のある 802.11r Fast Transition ワイヤレス クライアントが Fast Transition を使用可能になり、「概要」セクションにリストされている問題に対して脆弱になる恐れがあります。

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。

脆弱性を含んでいないことが確認された製品

この脆弱性に該当するその他の Cisco 製品は現在のところ見つかっていません。

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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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

次の表では、左側の列に主なソフトウェア リリースを記載しています。 右の列は、メジャー リリースが本アドバイザリに記載している脆弱性に該当するかどうか、また、本脆弱性に対する修正を含む最初のマイナー リリースに該当するかどうかを示します。

Cisco IOS アクセス ポイント 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修正リリース
Prior to 8.0	8.2.170.0
8.0	8.2.170.0
8.1	8.2.170.0
8.2	8.2.170.0
8.3	8.3.150.0
8.4	8.5.131.0
8.5	8.5.131.0
8.6	8.8.100.0
8.7	8.8.100.0
8.8	脆弱性なし
8.9	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-20190717-aironet-dos

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019 年 7 月 17 日

利用規約

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。