Cisco Aironet 1560、2800、および 3800 シリーズ アクセス ポイント プラットフォームでの 802.11 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-20171101-aironet1
初公開日 : 2017-11-01 16:00
最終更新日 : 2017-11-02 18:44
バージョン 1.1 : Final
CVSSスコア : 7.4
回避策 : No workarounds available
Cisco バグ ID : CSCve12189

CVE-2017-12273

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 Aironet 1560、2800、3800 シリーズ アクセス ポイントに対する 802.11 関連付け要求フレーム処理における脆弱性により、未認証のレイヤ 2 無線周波数（RF）近接攻撃者がアクセス ポイント（AP）のリロードを引き起こし、その結果、サービス妨害（DoS）状態が発生する可能性があります。

この脆弱性は、802.11 関連付け要求のフレーム検証が不十分であることに起因するものです。この脆弱性は、攻撃者がターゲット デバイスに不正な形式の 802.11 関連付け要求を送信することによって、不正利用される可能性があります。不正利用されると、攻撃者が AP のリロードを引き起こし、その結果、AP のリロード中に DoS 状態が発生す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。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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-aironet1

該当製品

脆弱性のある製品

この脆弱性は、Lightweight AP ソフトウェアまたは Mobility Express イメージのいずれかを実行している下記シスコ製品に影響します。

- Aironet 1560 シリーズ アクセス ポイント
- Aironet 2800 シリーズ アクセス ポイント
- Aironet 3800 シリーズ アクセス ポイント

注：Cisco Aironet 1560シリーズアクセスポイントデバイスは、リリース8.3.112.0からサポートされています。

ソフトウェア バージョンの判別

デバイスで実行されている Cisco Aironet シリーズ アクセス ポイント ソフトウェアのバージョンは、管理者がコントローラの Web インターフェイスまたは CLI を使用して確認することができます。

Web インターフェイスを使用する場合、Web インターフェイスにログインして、[管理（Management）] > [ソフトウェア アップデート（Software Update）] を選択し、ページの上部に表示されるリリース番号を参照します。

CLI を使用する場合は、 show version コマンドを実行し、出力結果の [AP 実行イメージ（AP Running Image）] フィールドの値を参照します。たとえばデバイスがソフトウェア バージョン 8.3.102.0 を実行している場合、コマンドの出力は次のようになります。

<#root>

```
AP# show version
.
.
.
cisco AIR-AP3802E-B-K9 ARMv7 Processor rev 1 (v7l) with 1030528/668540K bytes of memory.
Processor board ID RFDPP1BS497
AP Running Image     :

8.3.102.0

Primary Boot Image   : 8.3.102.0
.
.
.
```

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

シスコは、この脆弱性が Cisco Aironet 1800 シリーズ アクセス ポイントまたは Cisco IOS ソフトウェアを実行しているあらゆる Aironet アクセス ポイントに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。

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。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 http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

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、[シスコのセキュリティアドバイザリおよびアラート（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(http://www.cisco.com/en/US/support/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。

修正済みリリース

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。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-20171101-aironet1:Cisco Aironet 1560、2800、および3800シリーズアクセスポイントプラットフォームの802.11におけるDoS脆弱性
- cisco-sa-20171101-aironet2:Cisco Aironet 1560、2800、および3800シリーズアクセスポイントプラットフォームのExtensible Authentication Protocolにおけるサービス妨害(DoS)の脆弱性
- cisco-sa-20171101-wlc1:CiscoワイヤレスLANコントローラのSimple Network Management Protocolにおけるメモリリークによる DoS脆弱性
- cisco-sa-20171101-wlc2:Cisco Wireless LAN Controller 802.11v Basic Service Set Transition Managementのサービス妨害の脆弱性

次の表では、左の列にシスコ ソフトウェアのリリースを示しています。中央の列は、この脆弱性の修正が含まれた最初の推奨リリースです。右の列は、このアドバイザリ集で説明しているすべての脆弱性の修正が含まれた最初の推奨リリースです。

Cisco Aironet 1560、2800、3800 アクセス ポイント	この脆弱性に対して修正済みの推奨リリース	この脆弱および一連のアドバイザリに記載されているすべての脆弱性に関する推奨リリース
Prior to 8.0	該当なし	8.0.152.0
8.0	該当なし	8.0.152.0
8.1	該当なし	8.2.166.0
8.2	8.2.166.0	8.2.166.0
8.3	8.3.133.0	8.3.133.0
8.4	8.4.100.0	8.4.100.0
8.5	8.5.105.0	8.5.110.0（リリース予定）

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

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-20171101-aironet1

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	リリース 8.2 と 8.3 は、お客様の問題に対処するために再ビルドされました。推奨リリースが更新されました。	修正済みソフトウェア	Final	2017 年 11 月 2 日
1.0	初回公開リリース	—	Final	2017 年 11 月 1 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。