Cisco Aironet 1800、2800、および 3800 シリーズ アクセス ポイント プラグアンドプレイ 任意の コード実行脆弱性

High

アドバイザリーID : cisco-sa-20170503-cme

初公開日 : 2017-05-03 16:00

最終更新日 : 2017-09-21 16:44

バージョン 1.1 : Final

CVSSスコア : 7.5

回避策 : No workarounds available

Cisco バグ ID : CSCvb42386

CVE-2017-3873

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 1800 のプラグアンドプレイ（PnP）サブシステムの脆弱性は、2800、および Lightweight アクセスポイント（AP）を実行する 3800 シリーズ アクセス ポイントまたは Mobility Express な イメージ非認証、隣接した攻撃者が *ルート 特権*の任意 の コードを実行することを可能にする可能性があります。

脆弱性は PnP サーバレスポンスの不十分な検証が原因です。 PnP 機能はファクトリ リセットが発行された後がだけデバイスは設定が含まれていない初めて ブートのようなアクティブ、またはです。 影響を受けたデバイスからの PnP Configuration 要求に応答する機能の攻撃者は PnP 悪意のある応答を返すことによって脆弱性を不正利用できます。 Cisco Application Policy Infrastructure Controller エンタープライズ モジュール（APIC-EM）がネットワークで利用できる場合、攻撃者は有効な PnP 応答が受け取られた前に短いウィンドウの問題を不正利用する必要があります。 成功すれば、攻撃者はデバイスの基礎オペレーティング システムの *ルート 特権*の任意 の コードを実行する機能を得る可能性があります。

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-20170503-cme

該当製品

脆弱性のある製品

Cisco はこのアドバイザリのための唯一の脆弱 な ソフトウェア バージョンが Lightweight アクセス ポイント ソフトウェアか Mobility Express な イメージを実行する以下の製品の 8.3.102.0 であることを確認しました:

- Cisco Aironet 1800 シリーズ アクセス ポイント
- Cisco Aironet 2800 シリーズ アクセス ポイント
- Cisco Aironet 3800 シリーズ アクセス ポイント

Ciscoエアロネットシリーズ アクセス ポイント ソフトウェアのどのバージョンがデバイスで動作しているか判別するために、管理者はコントローラ Webインターフェイスか CLI を使用できます。

Webインターフェイスを、ログインは Webインターフェイスに使用するために、 **管理 > ソフトウェア アップデートを**選択し、次にページの上で現われるリリース番号を示します。

CLI を使用するために、 **show version コマンドを**発行し、次にコマンド 出力の **Image フィールドを実行する AP** の値を参照して下さい。 次の例はソフトウェア バージョン 8.3.102.0 を実行するデバイスのためのコマンドの出力を示したものです:

```
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

Cisco はこの脆弱性が IOS software を実行する Cisco Aironet アクセス ポイントを影響を与えないことを確認しました。

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。

侵害のインジケーター

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。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.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。
http://www.cisco.com/en/US/support/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

Cisco Aironet 1800、2800、3800 アクセス ポイント	この脆弱性に対する最初の修正リリース
Prior to 8.0	脆弱性なし
8.0	脆弱性なし
8.1	脆弱性なし
8.2	脆弱性なし
8.3	8.3.112.0（**注を**参照して下さい）
8.4	脆弱性なし

注-バージョン 8.3.111.0 は 8.3.112.0 によって最初の修正済み バージョンでが、延期され、取り替えられました。

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

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170503-cme

改訂履歴

Version	Description	Section	Status	日付
1.1	Metadata update.		Final	2017-September-21
1.0	Initial public release.		Final	2017-May-03

利用規約