Cisco Aironet 1830 Series and 1850 Series Access Points Mobility Express Default Credential Vulnerability

Critical

アドバイザリーID : cisco-sa-20170405-ame

初公開日 : 2017-04-05 16:00

最終更新日 : 2017-09-21 16:45

バージョン 1.4 : Final

CVSSスコア : 9.8

回避策 : No workarounds available

Cisco バグ ID : CSCva50691

CVE-2017-3834

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 Mobility Express ソフトウェアを実行する Cisco Aironet 1830 シリーズおよび Cisco Aironet 1850 シリーズ アクセス ポイントの脆弱性により、認証されていないリモート攻撃者が該当デバイスを完全に制御する可能性があります。

この脆弱性は、Cisco Mobility Express ソフトウェアを実行する該当デバイスにデフォルトのクレデンシャルが存在することに起因します。これは、デバイスがマスター、下位、スタンドアロンのどのアクセス ポイントとして構成されているかには関係しません。 該当デバイスにレイヤ 3 接続できる攻撃者は、セキュア シェル（SSH）を使用して該当デバイスに昇格された特権を使用してデバイスにログインする可能性があります。 不正利用に成功すると、攻撃者はデバイスを完全に制御す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-20170405-ame

該当製品

脆弱性のある製品

この脆弱性は、Cisco Mobility Express ソフトウェアの 8.2.121.0 より前の 8.2.x リリースを実行する Cisco Aironet 1830 シリーズおよび Cisco Aironet 1850 シリーズ アクセス ポイントに影響を与えます。これは、デバイスがマスター、下位、スタンドアロンのどのアクセス ポイントとして構成されているかには関係しません。 リリース 8.2 は、次世代 Cisco Aironet アクセス ポイント向け Cisco Mobility Express ソフトウェアの最初のリリースです。

デバイス上で実行されている Cisco Mobility Express ソフトウェアのリリースは、管理者が Cisco Mobility Express ワイヤレス 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。

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、 **show version** コマンドを発行して、コマンドの出力を参照します。 次に、Cisco Mobility Express Software Release 8.3.111.0 を実行する Cisco Aironet 1852i アクセス ポイントでのコマンド出力例を示します。

```
AP# show version

cisco AIR-AP1852I-UXK9 ARMv7 Processor rev 0 (v71) with 997184/525160K bytes of memory.
Processor board ID RFDP2BCR021
AP Running Image : 8.3.111.0
Primary Boot Image : 8.3.111.0
Backup Boot Image : 8.1.106.33
AP Image type : MOBILITY EXPRESS IMAGE
AP Configuration : MOBILITY EXPRESS CAPABLE
.
.
```

.このデバイスはこの脆弱性の影響を受けません。

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、Cisco Lightweight アクセス ポイント（AP）ソフトウェアまたは Cisco IOS ソフトウェアを実行する Cisco Aironet アクセス ポイントには影響を与えないことを確認しました。

また、シスコはこの脆弱性が以下のシスコ製品には影響を与えないことを確認しました。いかの

- Cisco Mobility Express ソフトウェアを実行している Aironet 2800 シリーズ アクセス ポイント
- Cisco Mobility Express ソフトウェアを実行している Aironet 3800 シリーズ アクセス ポイント
- ワイヤレス コントローラ（すべての Cisco モデル）
- ワイヤレス LAN コントローラ（すべての Cisco モデル）

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

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-20170405-ame： Cisco Aironet 1830 Series and 1850 Series Access Points Mobility Express Default Credential Vulnerability
- cisco-sa-20170405-wlc： Cisco Wireless LAN Controller 802.11 WME Denial of Service Vulnerability
- cisco-sa-20170405-wlc2： Cisco Wireless LAN Controller IPv6 UDP Denial of Service Vulnerability
- cisco-sa-20170405-wlc3： Cisco Wireless LAN Controller Management GUI Denial of Service Vulnerability

次の表では、左の列にシスコ ソフトウェアのメジャー リリースを示します。 中央の列が示すのは、本アドバイザリに記載された脆弱性によるメジャー リリースへの影響の有無、また、本脆弱性に対する修正を含む最初のマイナー リリースです。 右の列が示すのは、一連のアドバイザリに記載された脆弱性によるメジャー リリースへの影響の有無、およびそれらの脆弱性に対する最新の推奨リリースです。

Cisco Mobility Express Software Major Release	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
Prior to 8.0	脆弱性なし	8.0.140.0
8.0	脆弱性なし	8.0.140.0
8.1	脆弱性なし	8.2.130.0
8.2	8.2.121.0	8.2.141.0
8.3	脆弱性なし	8.3.112.0
8.4	脆弱性なし	8.4.100.0 (future release)

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

この問題は、カスタマー サポート ケースの解決中に Cisco TAC によって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ame

改訂履歴

Version	Description	Section	Status	日付
1.4	Metadata update.		Final	2017-September-21

1.3	Metadata update.		Final	2017-September-13
1.2	Metadata update.		Final	2017-September-11
1.1	Updated first fixed software release for 8.2 from 8.2.111.0 to 8.2.121.0.	Vulnerable Products and Fixed Software.	Final	2017-May-30
1.0	Initial public release.		Final	2017-April-05

利用規約