Cisco Mobility Express 1800 のアクセス ポイント シリーズ 認証 バイパス の 脆弱性

Critical

アドバイザリーID : cisco-sa-20170315-ap1800
初公開日 : 2017-03-15 16:00
最終更新日 : 2017-10-06 14:32
バージョン 1.3 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID : CSCuy68219

CVE-2017-3831

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 1800 シリーズ アクセス ポイントの Webベース GUI の脆弱性はリモート攻撃者非認証が認証をバイパスするようにする可能性があります。 攻撃者は完全なアドミニストレーター特権を許可できます。

脆弱性は GUIインターフェイスを使用してある特定の Webページにアクセスするための認証の不適当な実装が原因です。 攻撃者は影響を受けたシステムの Webインターフェイスへ巧妙に細工された HTTP 要求を送信 することによってこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者が認証をバイパスし、影響を受けたデバイスへの無許可の設定変更か問題制御指令を実行することを可能に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-20170315-ap1800

該当製品

脆弱性のある製品

この脆弱性は 8.2.110.0 前にソフトウェア バージョンを実行する Cisco Mobility Express 1800 シリーズ アクセス ポイントに影響を与えます。 どのソフトウェア 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 Webインターフェイスを使用するか、または CLI からの **show version コマンドを**発行できます。 この例では、デバイスはソフトウェア バージョン 8.1.10.159 を実行しています。

```
# show version
Cisco AP Software, (ap1g4), [cheetah-build:/local/build/JENKINS/workspace/Nightly-Cheetah-
corsica-v8_1_throttle-cco]
Technical Support:  http://www.cisco.com/techsupport Copyright (c) 1986-2015 by Cisco Systems,
Inc.
Compiled Thu Jul 23 09:45:56 PDT 2015

ROM: Bootstrap program is U-Boot boot loader
BOOTLDR: U-Boot boot loader Version 17
AP38ED.18CC.1C20 uptime is 0 days, 0 hours, 1 minutes
Last reload time   : Thu Oct 22 04:07:54 UTC 2015
Last reload reason : capwapd triggered reboot
cisco AIR-AP1852E-Z-K9 ARMv7 Processor rev 0 (v7l) with 997184/802540K bytes of memory.
Processor board ID KWC192900P1
AP Image version (active)  : 8.1.10.159
.
.
.
```

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。

- Mobility Express な 2800 シリーズ アクセス ポイント
- Mobility Express な 3800 シリーズ アクセス ポイント

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

次の表に示すように、適切なリリースにアップグレードする必要があります。

Mobility Express な 1800 シリーズ アクセス ポイント メジャーリリース	First Fixed Release（修正された最初のリリース）
8.1	影響あり。 8.2.130.0 またはそれ以降への移行する
8.2	8.2.130.0 またはそれ以降
8.3	脆弱性なし

注: Cisco ソフトウェアのダウンロード ページから延期された最初の修正済みソフトウェアリリースは 8.2.110.0 でした。 8.2.130.0 またはそれ以降 ソフトウェア リリースは使用する必要があります。

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

Cisco はこの脆弱性を発見することおよび報告するために Rigo Information Technology のセキュリティ研究者に感謝することを Bijay Limbu Senihang 望みます。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-ap1800

改訂履歴

Version	Description	Section	Status	日付
1.3	Metadata update.		Final	2017-October-06
1.2	Metadata update.		Final	2017-September-27
1.1	Metadata update.		Final	2017-September-21
1.0	Initial public release.		Final	2017-March-15

利用規約