Cisco はワイヤレス LAN コントローラ偽装脆弱性を一致させました

High

アドバイザリーID : cisco-sa-20170315-wlc-mesh

初公開日 : 2017-03-15 16:00

最終更新日 : 2017-10-06 14:32

バージョン 1.1 : Final

CVSSスコア : 8.8

回避策 : No workarounds available

Cisco バグ ID : CSCuu14804 CSCuc98992

CVE-2017-3854

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ワイヤレス LAN コントローラ (WLC) ソフトウェアのメッシュ コードの脆弱性はリモート攻撃者非認証がメッシュ トポロジーの WLC に扮するようにする可能性があります。

脆弱性はメッシュ 設定の親アクセス ポイントの不十分な認証が原因です。 攻撃者はターゲット システムの強制によって正しい親アクセス ポイントから切り離し、攻撃者が所有した不正なアクセス ポイントに再接続するためにこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者がトラフィック フローを影響を与えられたアクセス ポイントを通して制御するか、またはターゲット システムの完全 な 制御を引き継ぐ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。 追加設定が修正済みリリースへのアップグレードに加えて必要であることに注目して下さい。 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-wlc-mesh

該当製品

脆弱性のある製品

この脆弱性は脆弱なバージョンをワイヤレス LAN コントローラ ソフトウェアのおよび設定される実行する以下の製品に一致させたモードのために影響を及ぼします:

- Cisco 8500 シリーズ ワイヤレス コントローラ
- Cisco 5500 シリーズ ワイヤレス コントローラ
- Cisco 2500 シリーズ ワイヤレス コントローラ
- Cisco Flex 7500 シリーズ ワイヤレス コントローラ
- Cisco Virtual Wireless Controller
- Wireless Services Module 2（WiSM2）（WiSM2）

該当するリリースに関する詳細についてはこの Security Advisory の「修正済みソフトウェア」セクションを参照して下さい。

WLC が一致させたモードのために設定されるかどうか判別するために、 **show ap config general コマンドを**使用し、 *APモードが繋ぐために*設定 されることを確認して下さい。 次の例は一致させたモードのために設定される WLC を示したものです:

```
Cisco AP Identifier.............................. 23
Cisco AP Name.................................... ap1

[...]
AP Mode ..................................... Bridge
AP Role ..................................... RootAPCisco AP
Identifier.............................. 23
Cisco AP Name.................................... ap1

[...]
AP Mode ..................................... Bridge
AP Role ..................................... RootAP
```

注： 一致させたモードはデフォルトで有効に なりません。

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。

以下の製品はこの脆弱性から影響を受けません:

- Cisco Catalyst 3850 シリーズ スイッチの統合されたコントローラ
- Cisco Catalyst 3650 シリーズ スイッチの統合されたコントローラ
- Cisco Mobility Express
- Cisco 5760 ワイヤレス LAN コントローラ

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。

Cisco WLC メジャーリリース	First Fixed Release (修正された最初のリリース)
Prior to 8.0	影響あり。 8.0.140.0 およびそれ以降[1] への移行する
8.0	8.0.140.0 およびそれ以降[1]

8.1	影響あり。 8.2 またはそれ以降[1] への移行する
8.2	影響を受けなかった[1]
8.3	影響を受けなかった[1]

[1] つの**注記:** 修正されたコードへのアップデートの後で、管理者はまたメッシュ 設定のための認証を設定する必要があります。 次のリソースは方法で情報をこの機能を設定する提供します: http://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-3/b_mesh_83/Connecting_the_Cisco_1500_Series_Mesh_Access_Points_to_the___.html#concept_D2BB5214172F45AE8ADE17415811C67D

メッシュ 設定のための認証は修正済みリソースだけで利用できます。

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

この脆弱性はサポート ケースの解決の間に発見されました。

URL

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

改訂履歴

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

利用規約