Cisco Wireless LAN Controller 802.11 WME Denial of Service Vulnerability

アドバイザリーID : cisco-sa-20170405-wlc CVE-2016-9194
初公開日 : 2017-04-05 16:00
最終更新日 : 2017-10-06 14:32
バージョン 1.1 : Final
CVSSスコア : 7.4
回避策 : No workarounds available
Cisco バグ ID : CSCva86353

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 Wireless LAN Controller(WLC)ソフトウェアの802.11 Wireless Multimedia Extensions(WME)アクションフレーム処理の脆弱性により、認証されていない隣接する攻撃者がサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、802.11 WMEパケットヘッダーの不完全な入力検証に起因します。攻撃者は、不正な形式の802.11 WMEフレームをターゲットデバイスに送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はWLCの予期しないリロードを引き起こす可能性があります。

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-20170405-wlc

該当製品

脆弱性のある製品

この脆弱性は、Cisco Wireless LAN Controllerに影響します。該当するソフトウェア リリースについては、このアドバイザリの「修正済みソフトウェア」の項を参照してください。

デバイスで実行されている Cisco WLC ソフトウェアのリリースを確認するには、管理者は

Web インターフェイスか CLI を使用します。

Web インターフェイスを使用する場合は、Web インターフェイスにログインして Monitor タブをクリックし、次に左ペインの Summary をクリックします。[ソフトウェア バージョン（ Software Version)] フィールドに、デバイスで現在実行されているソフトウェアのリリース番号が表示されます。

CLI を使用する場合は、 show sysinfo コマンドを実行し、次にコマンド出力の Product Version フィールドの値を参照して下さい。次の例は Cisco WLC ソフトウェア リリース 8.3.102.0 を実行するデバイスのコマンド出力を示したものです。

```
<#root>

(5500-4) >

show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.3.102.0
Bootloader Version............................... 1.0.1
Field Recovery Image Version..................... 6.0.182.0
Firmware Version................................. FPGA 1.3, Env 1.6, USB console 1.27
Build Type....................................... DATA + WPS
.
.
.
```

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。

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(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-20170405-ame:Cisco Aironet 1830シリーズおよび1850シリーズアクセスポイントのMobility Expressにおけるデフォルトクレデンシャルの脆弱性
- cisco-sa-20170405-wlc:CiscoワイヤレスLANコントローラ802.11 WMEのDoS脆弱性
- cisco-sa-20170405-wlc2:CiscoワイヤレスLANコントローラのIPv6 UDPにおけるDoS脆弱性
- cisco-sa-20170405-wlc3:CiscoワイヤレスLANコントローラ管理GUIのDoS脆弱性

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 ワイヤレス LAN コントローラ	この脆弱性に対する最初の修正リリース	この脆弱およびー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	脆弱性あり、8.0.140.0に移行	8.0.140.0
8.0	8.0.140.0	8.0.140.0
8.1	脆弱性あり、8.2.130.0に移行	8.2.141.0
8.2	8.2.130.0	8.2.141.0
8.3	8.3.111.0	8.3.112.0
8.4	脆弱性なし	8.4.100.0 (future release)

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 TAC のサポート案件の対応時に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-wlc

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	Metadata update.	—	Final	2017年10月6日
1.0	初回公開リリース	—	Final	2017 年 4 月 5 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。