Cisco Wireless LAN Controller 802.11 WME Denial of Service Vulnerability

High

アドバイザリーID : cisco-sa-20170405-wlc
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

CVE-2016-9194

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

802.11 Ciscoワイヤレス LAN コントローラ（WLC）ソフトウェアのワイヤレス マルチメディア拡張機能（WME）操作フレーム処理の脆弱性は非認証、隣接した攻撃者によりサービス拒否（DoS）状態を引き起こすことを可能にする可能性があります。

脆弱性は 802.11 WME パケットヘッダーの不完全な入力の検証が原因です。 攻撃者は目標とされたデバイスへ不正 な 802.11 WME 帯を送信 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により WLC は予想に反してリロードします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-20170405-wlc

該当製品

脆弱性のある製品

この脆弱性は Ciscoワイヤレス LAN コントローラに影響を与えます。 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。

Cisco WLC ソフトウェアのどのリリース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、 **Monitor タブ**をクリックし、次に左ペインの **要約を**クリックします。 **ソフトウェア バージョン** フィールドは現在 デバイスで動作するソフトウェアのリリース番号を示します。

CLI を使用するために、 **提示 sysinfo** コマンドを発行し、次にコマンド 出力の **製品 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ためのコマンドの出力を示したものです:

```
(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。

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ワイヤレス	この脆弱性に対する最初の修正リリース	この脆弱および一連のアドバイザリに記載

LAN コントローラ		
Prior to 8.0	脆弱性あり; 8.0.140.0 への移行する	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 への移行する	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)

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 Cisco TACサポート例の解決の間に発見されました。

URL

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

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-April-05

利用規約