シスコ ワイヤレス LAN コントローラ ソフトウェアで確認されたクロスサイト リクエスト フォージェリ（CSRF）の脆弱性

High

アドバイザリーID : cisco-sa-20190417-wlc-csrf

初公開日 : 2019-04-17 16:00

バージョン 1.0 : Final

CVSSスコア : 8.1

回避策 : No workarounds available

Cisco バグ ID : CSCvj06910

CVE-2019-1797

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

シスコ ワイヤレス LAN Controller（WLC）ソフトウェアの Web 管理インターフェイスでは脆弱性が発見されました。認証されていないリモートの攻撃者がクロスサイト リクエスト フォージェリ（CSRF）攻撃を仕掛け、ユーザの権限で任意の操作（デバイス構成を変更するなど）を実行できる危険性があります。

この脆弱性は、該当デバイス上の Web ベース管理インターフェイスの CSRF 防御が不十分であることに起因しています。 攻撃者は、細工されたリンクをインターフェースのユーザにクリックさせることで脆弱性をエクスプロイトできる可能性があります。 攻撃者がエクスプロイトに成功すると、該当ユーザの特権レベルで任意の操作を実行できる可能性があります。

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ました。 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-20190417-wlc-csrf

該当製品

脆弱性のある製品

今回の脆弱性は、脆弱なリリースのシスコ ワイヤレス LAN コントローラ（WLC）ソフトウェ

アを実行している Cisco WLC に影響します。

脆弱性が存在する Cisco WLC ソフトウェア リリースの情報については、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 リリースの判別

デバイスで実行されている Cisco WLC ソフトウェア リリースは、コントローラの Web インターフェイスまたは CLI から確認できます。

Web インターフェイスを使用する場合は、次を実行します。

1. ブラウザを使用して、コント ローラの Web インターフェイスにログインします。
2. [モニタ（Monitor）] タブをクリックします。
3. 左ペインで、[Summary（サマリ）] をクリックします。
4. [コントローラサマリ（Controller Summary）] の下にある [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 Telnet を使用してコントローラにログインして、**show sysinfo** コマンドを実行し、出力結果の **Product Version** フィールドの値を参照します。 たとえばデバイスが Cisco WLC ソフトウェア リリース 8.3.102.0 を実行している場合、コマンドの出力は次のようになります。

```
(wlc)> 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

このアドバイザリの脆弱性が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

詳細

詳細については、「 クロスサイト リクエスト フォージェリ（CSRF）の脅威について理解する」を参照してください。

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。 https://www.cisco.com/c/en/us/products/end-user-license-agreement.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。
https://www.cisco.com/c/en/us/support/web/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-20190417-aironet-shell： Cisco Aironet シリーズのアクセス ポイントで確認された

、開発シェルへのアクセスを許す脆弱性
- cisco-sa-20190417-wlc-csrf： シスコ ワイヤレス LAN コントローラ ソフトウェアで確認されたクロスサイト リクエスト フォージェリ（CSRF）の脆弱性
- cisco-sa-20190417-wlc-gui： シスコ製ワイヤレス LAN コントローラ用ソフトウェアの GUI 機能で発見されたサービス拒否の脆弱性
- cisco-sa-20190417-wlc-iapp： シスコ製ワイヤレス LAN コントローラ用ソフトウェアの IAPP メッセージ処理機能で発見されたサービス拒否の脆弱性

次の表では、左側の列に主なソフトウェア リリースを記載しています。 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。 右の列は、メジャー リリースがこのコレクションのアドバイザリに記載した何らかの脆弱性に該当するかどうか、また、これらすべての脆弱性に対する修正を含む最初のリリースを示します。

Cisco Wireless LAN Controller ソフトウェア

Cisco ワイヤレス LAN コントローラ メジャー ソフトウェア リリース	この脆弱性に対する最初の修正リリース	このアドバイザリ集で説明している脆弱性すべてに対する推奨リリース
8.0[1] 前	8.3.150.0	8.3.150.0
8.0[1]	8.3.150.0	8.3.150.0
8.1[1]	8.3.150.0	8.3.150.0
8.2[1]	8.3.150.0	8.3.150.0
8.3	8.3.150.0	8.3.150.0
8.4	8.5.135.0	8.5.140.0
8.5	8.5.135.0	8.5.140.0
8.6	8.8.100.0	8.8.120.0
8.7	8.8.100.0	8.8.120.0
8.8	8.8.100.0	8.8.120.0
8.9	脆弱性なし	脆弱性なし

1. CSRF 攻撃への対策が最初に施されたのはソフトウェア リリース 8.3 です。

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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-wlc-csrf

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019 年 4 月 17 日

利用規約