シスコ ワイヤレス LAN コントローラ ソフトウェア GUI の特権昇格の脆弱性

High

アドバイザリーID : cisco-sa-20181017-wlc-gui-privesc

初公開日 : 2018-10-17 16:00

バージョン 1.0 : Final

CVSSスコア : 7.5

回避策 : No workarounds available

Cisco バグ ID : CSCvh65876

CVE-2018-0417

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 コントローラ（WLC）ソフトウェアを使用する TACACS 認証の脆弱性によって、認証済みのローカルの攻撃者が、通常 CLI では利用できない特定の操作を GUI で行えるようになる可能性があります。

この脆弱性は、リモートの TACACS サーバの応答によって受信した特定の TACACS 属性が誤って構文解析されることで発生します。 攻撃者がこの脆弱性を不正利用して、TACACS 認証により該当デバイスの GUI にアクセスする可能性があります。 これに成功すると、管理者権限を持つローカル ユーザ アカウントを該当の WLC に作成し、CLI では許可されない、禁止すべきその他のコマンドを実行するおそれがあります。

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-20181017-wlc-gui-privesc

該当製品

脆弱性のある製品

最初の修正済みリリースより前のソフトウェア リリースを実行中で、TACACS 認証を設定したシスコ ワイヤレス LAN コントローラがこの脆弱性の影響を受けます。 TACACS 認証が設

定されていない場合、WLC は脆弱ではありません。

TACACS 認証が設定されているかどうかの判定

show tacacs-server の機能が利用できない場合、つまり TACACS の機能（feature tacacs）が有効ではない場合、そのデバイスは、この脆弱性の影響を受けません。 次の例で、デバイスが脆弱であるかどうかを管理者が確認できる出力結果を示します。

show tacas summary コマンドを発行後、表の下に何も表示されない場合、そのデバイスは TACACS サービスを実行していないため、脆弱ではありません。 次の例で、TACACS サービスを実行している脆弱なデバイスの出力結果を示します。

```
(wlc) >show tacacs summary
Authentication Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2

Authorization Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2

Accounting Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2
```

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、管理者がコントローラの Web インターフェイスまたは CLI を使用して確認することができます。

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. 左側のペインで [概要（Summary）] をクリックします。
4. [コントローラの概要（Controller Summary）] の [ソフトウェア バージョン（Software Version）] フィールドは、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を示します。

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のある製品セクションに記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

回避策

この脆弱性に対処する回避策はありません。 緩和策として、お客様は、アクセス コントロール リスト（ACL）を実装してフィルタリングしたり、設定済みデバイスへの管理アクセスを制限したりすることができます。

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が新規リリースで引き続き正しくサポートされていることを十分に確認してください。 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

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-20181017-wlc-gui-privesc: シスコ ワイヤレス LAN コントローラ ソフトウェア GUI の特権昇格の脆弱性
- cisco-sa-20181017-ap-ft-dos: Cisco IOS アクセス ポイント ソフトウェア 802.11r Fast Transition におけるサービス妨害（DoS）の脆弱性
- cisco-sa-20181017-wlc-capwap-memory-leak: シスコ ワイヤレス LAN コントローラ ソフトウェア Control and Provisioning of Wireless Access Points プロトコルにおける情報漏えいの脆弱性
- cisco-sa-20181017-wlc-capwap-dos: シスコ ワイヤレス LAN コントローラ ソフトウェア Control and Provisioning of Wireless Access Points プロトコルにおけるサービス妨害の脆弱性

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。 次の表で、左の列は、シスコ ソフトウェアのメジャー リリースを、中央の列は、この脆弱性に対処する修正を含む最初のマイナー リリースを示します。 また、右の列は、この脆弱性への対処としてインストールを推奨するリリースを示します。

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	この脆弱性のための推奨リリース
Prior to 8.0	8.2.170.0	8.2.170.0
8.0	8.2.170.0	8.2.170.0
8.1	8.2.170.0	8.2.170.0
8.2	8.2.170.0	8.2.170.0
8.3	TAC より入手可能 1	TAC より入手可能 1
8.4	8.5.131.0	8.5.135.0
8.5	8.5.131.0	8.5.135.0
8.6	8.7.102.0	8.7.106.0
8.7	8.7.102.0	8.7.106.0

8.8	脆弱性なし	脆弱性なし

1 8.3 メンテナンス リリース 4 のエスカレーション イメージは、ご希望に応じて、Cisco TAC から入手可能です。

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-20181017-wlc-gui-privesc

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-October-17

利用規約