Cisco Small Business スイッチで確認された情報開示の脆弱性

High

アドバイザリーID : cisco-sa-20200129-smlbus-switch-disclos

初公開日 : 2020-01-29 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 : CSCvr54104 CSCvs68748

CVE-2019-15993

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 Small Business スイッチの Web UI で確認された脆弱性により、認証されていないリモートの攻撃者が機密のデバイス情報にアクセスする可能性があります。

この脆弱性は、Web UI からアクセス可能な情報に対してソフトウェアで適切な認証制御が行われていないことが原因で発生します。 攻撃者は、該当デバイスの Web UI に悪意のある HTTP 要求を送信することにより、この脆弱性をエクスプロイトする可能性があります。 エクスプロイトが成功すると、攻撃者は設定ファイルを含む機密のデバイス情報にアクセスす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-20200129-smlbus-switch-disclos

該当製品

脆弱性のある製品

この脆弱性の影響を受けるのは、次のシスコ製品で 2.5.0.92 よりも前のファームウェア リリースを実行している場合です。

- 250 シリーズ スマート スイッチ
- 350 シリーズ マネージド スイッチ
- 350X シリーズ スタッカブル マネージド スイッチ
- 550X シリーズ スタッカブル マネージド スイッチ

この脆弱性の影響を受けるのは、次のシスコ製品で 1.4.11.4 よりも前のファームウェア リリースを実行している場合です。

- 200 シリーズ スマート スイッチ
- 300 シリーズ マネージド スイッチ
- 500 シリーズ スタッカブル マネージド スイッチ

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

回避策

この脆弱性に対処する回避策はありません。

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

ファームウェアリリース 2.5.0.92 のこの脆弱性は、以下のシスコ製品で修正されています。

- 250 シリーズ スマート スイッチ
- 350 シリーズ マネージド スイッチ
- 350X シリーズ スタッカブル マネージド スイッチ
- 550X シリーズ スタッカブル マネージド スイッチ

ファームウェアリリース 1.4.11.4 のこの脆弱性は、以下のシスコ製品で修正されています。

- 200 シリーズ スマート スイッチ
- 300 シリーズ マネージド スイッチ
- 500 シリーズ スタッカブル マネージド スイッチ

Cisco.com の Software Center からファームウェアをダウンロードするには、以下の手順を実行します。

1. [すべて参照（Browse all）] をクリックします。
2. [スイッチ（Switches）] > [LANスイッチ（LAN Switches）] > [Small Business] の順に選択します。
3. 製品セレクタの右ペインから特定の製品を選択します。
4. **スマートスイッチファームウェア**または**スイッチファームウェア**を選択します。
5. ページの左ペインからリリースを選択します。

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

この脆弱性を報告していただいた DFDR Consulting LLC 社の Ken Pyler 氏に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200129-smlbus-switch-disclos

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	2020 年 1 月 29 日

利用規約

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。