

Cisco Small Business 220シリーズスマートスイッチの認証バイパスの脆弱性

Critical アドバイザリーID : cisco-sa-20190806-sb220-auth_bypass [CVE-2019-1912](#)
初公開日 : 2019-08-06 14:00
最終更新日 : 2019-08-21 14:24
バージョン 1.1 : Final
CVSSスコア : [9.1](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCvo78300](#)

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 220シリーズスマートスイッチのWeb管理インターフェ이스の脆弱性により、認証されていないリモートの攻撃者が任意のファイルをアップロードできる可能性があります。

この脆弱性は、Web管理インターフェ이스での認証チェックが不完全であることに起因します。攻撃者は、Web管理インターフェ이스の特定の部分に悪意のある要求を送信することで、この脆弱性を不正利用する可能性があります。影響を受けるスイッチの設定に応じて、悪意のある要求はHTTPまたはHTTPS経由で送信される必要があります。エクスプロイトに成功すると、攻撃者は該当デバイスの設定を変更したり、逆シェルを挿入したり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。

このアドバイザリーは、次のリンクより確認できます。

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-auth_bypass

該当製品

脆弱性のある製品

この脆弱性は、Web 管理インターフェイスが有効になっている、1.1.4.4 より前のファームウェアバージョンを実行中の Cisco Small Business 220 シリーズ スマート スイッチに影響を及ぼします。Web 管理インターフェイスは、デフォルトでは HTTP 経由と HTTPS 経由の両方で有効になっています。

Web 管理インターフェイスが有効になっているかどうかの確認

Web 管理インターフェイスが HTTP 経由と HTTPS 経由の両方で有効になっているかどうかを確認するため、管理者は、デバイス CLI で `show running-config http` コマンドを使用できます。次の両方の行が設定に含まれている場合、Web 管理インターフェイスは無効になっており、デバイスに脆弱性はありません。

```
no ip http server no ip http secure server
```

その他の出力は、デバイスで Web 管理インターフェイスが有効になっていることを示します。

Web 管理インターフェイスの [セキュリティ (Security)] > [TCP/UDPサービス (TCP/UDP Service)] で [HTTPサービス (HTTP Service)] と [HTTPSサービス (HTTPS Service)] を設定できます。

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。

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です。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 Cisco Service Contract 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 POS 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

この脆弱性は、Cisco 220 シリーズ スマート スイッチ ファームウェア リリース 1.1.4.4 以降で修正されています。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT; プロダクト セキュリティ インシデント レスポンス チーム) は、公開されているエクスプロイト コードの存在を認識しています。このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

出典

シスコは、VDOO Disclosure Program を通してこの脆弱性を報告して下さったセキュリティ研究者 Bashis 氏に感謝いたします。

URL

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	エクスプロイトコードの入手状況に関する情報を追加。	不正利用事例と公式発表	Final	2019年8月21日
1.0	初回公開リリース	-	Final	2019年8月6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、単独の転載や意識を施した場合、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。