Cisco Small Business 220 シリーズ スマートスイッチの脆弱性

アドバイザリーID : cisco-sa-ciscosb-multivulns-Wwyb7s5E
初公開日 : 2021-06-16 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 : CSCvx57935 CSCvx57925 CSCvx57830

CVE-2021-1571
CVE-2021-1542
CVE-2021-1541
CVE-2021-1543

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 ベース管理インターフェイスに複数の脆弱性が存在するため、攻撃者が次のことを行う可能性があります。

- ユーザーセッションのハイジャック
- ルートユーザ–として基盤となるオペレーティングシステムで任意のコマンドを実行
- クロスサイト スクリプティング（XSS）攻撃
- HTML インジェクション攻撃

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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。これら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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E

該当製品

脆弱性のある製品

これらの脆弱性は、リリース 1.2.0.6 より前のファームウェアリリースを実行しており、Web ベースの管理インターフェイスが有効になっている 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 ベースの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 ベースの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 ベースの管理インターフェイスが HTTP 経由や HTTPS 経由で有効になっているかどうかを確認するには、デバイス CLI で show running-config コマンドを使用します。次の両方の行が設定に含まれている場合、Web ベースの管理インターフェイスは無効になっており、そのデバイスは影響を受けません。

<#root>

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

その他の出力は、デバイスで Web ベースの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 ベース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、これらの脆弱性の影響を受けることが分かっています。

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2021-1542:Cisco Small Business 220シリーズスマートスイッチの脆弱なセッション管理の脆弱性

Cisco Small Business シリーズ スマートスイッチの Web ベース管理インターフェイスのセッション管理に脆弱性が存在するため、認証されていないリモート攻撃者が認証保護をバイパスして、管理インターフェイスに不正アクセスする可能性があります。攻撃者は、ハイジャックしたセッションアカウントの権限を取得できる可能性があります。これには、デバイスの管理者権限が含まれます。

この脆弱性は、セッション識別子の値に対して使用するセッション管理が脆弱であることに起因します。偵察によって有効なセッション ID を作成する方法が特定されると、この脆弱性がエクスプロイトされる可能性があります。エクスプロイトに成功すると、攻撃者は管理者ユーザーのレベルまで権限を昇格させて、管理インターフェイス内でアクションを実行できるようになります。

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。

バグID:CSCvx57925
CVE ID：CVE-2021-1542
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.5
CVSSベクトル：CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

CVE-2021-1541:Cisco Small Business 220シリーズスマートスイッチのリモートコマンド実行の脆弱性

Cisco Small Business 220 シリーズ スマートスイッチの Web ベース管理インターフェイスの脆弱性により、認証されたリモートの攻撃者が、ルートユーザーとして基盤となるオペレーティングシステムで任意のコマンドを実行する可能性があります。攻撃者は、デバイスに対する有効な管理者用のログイン情報を有している必要があります。

この脆弱性は、TFTP 設定パラメータの検証が行われないことに起因します。特定の TFTP 設定パラメータの入力が細工されると、この脆弱性がエクスプロイトされる可能性があります。エクスプロイトに成功すると、攻撃者は基盤となるオペレーティングシステム上でルートユーザーとして任意のコマンドを実行できるようになります。

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。

バグID:CSCvx57935
CVE ID：CVE-2021-1541
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.2
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVE-2021-1543:Cisco Small Business 220シリーズスマートスイッチのクロスサイトスクリプティング(XSS)の脆弱性

Cisco Small Business 220 シリーズ スマートスイッチの Web ベース管理インターフェイスの脆弱性により、認証されていないリモートの攻撃者がクロスサイト スクリプティング（XSS）攻撃を実行する可能性があります。

この脆弱性は、該当デバイスの Web ベースの管理インターフェイスでユーザーが行った入力の検証が不十分であることに起因します。攻撃者は、ユーザーが悪意のあるリンクをクリックして、特定のページにアクセスするように誘導することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は影響を受けるインターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセスして、ユーザーを任意のページにリダイレクトしたりできるようになります。

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。

バグID:CSCvx57830
CVE ID：CVE-2021-1543
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.1
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVE-2021-1571:Cisco Small Business 220シリーズスマートスイッチにおけるHTMLインジェクションの脆弱性

Cisco Small Business 220 シリーズ スマートスイッチの Web ベース管理インターフェイスの脆弱性により、認証されていないリモートの攻撃者が HTML インジェクション攻撃を実行する可能性があります。

この脆弱性は、影響を受けるページのパラメータ値の検証が不適切であることに起因します。攻撃者はユーザーを誘導して、細工されたリンクに従って、HTML コードを該当パラメータに送らせることで、脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は Web ページのコンテンツを改ざんして、悪意が潜む Web サイトにユーザーをリダイレクトできるようになります。

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。

バグID:CSCvx57830
CVE ID：CVE-2021-1571
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.1
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

回避策

これら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、シスコ セキュリティ アドバイザリ 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アップグレード ソリューション一式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（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

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

Cisco Small Business 220 シリーズ スマート スイッチ ファームウェア リリース 1.2.0.6 以降では、この脆弱性は修正されています。

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、[すべて参照（Browse all）] をクリックし、[スイッチ（Switches）] > [LAN スイッチ - スモールビジネス（LAN Switches - Small Business）] の順に移動します。

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とその公表は確認しておりません。

出典

これらの脆弱性を報告していただいたセキュリティ研究者の Jasper Lievisse 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2021 年 6 月 16 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。