Cisco Small Businessシリーズスイッチのスタックリロードにおける ACLバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-sb-bus-acl-bypass-5zn9hNJk
CVE-2024-20263
初公開日 : 2024-01-24 16:00
バージョン 1.0 : Final
CVSSスコア : 5.8
回避策 : No workarounds available
Cisco バグ ID : CSCwh68993 CSCwf48882

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 Business 250シリーズスマートスイッチおよびBusiness 350シリーズマネージドスイッチのスタックスイッチ設定内のアクセスコントロールリスト(ACL)管理に関する脆弱性により、認証されていないリモートの攻撃者が該当デバイスに設定されたACLによる保護をバイパスできる可能性があります。

この脆弱性は、プライマリスイッチまたはバックアップスイッチでスタック全体のリロードまたは電源の再投入が発生したときに、スタック構成でACLが正しく処理されないことに起因します。攻撃者は、該当デバイスを介して巧妙に細工されたトラフィックを送信することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は設定されたACLをバイパスし、トラフィックが予期せぬ方法でドロップまたは転送される可能性があります。攻撃者は、デバイスが脆弱な状態になる条件を制御できません。

注：脆弱性のある状態では、ACLはプライマリデバイスに正しく適用されますが、バックアップデバイスに正しく適用されない可能性があります。

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-sb-bus-acl-bypass-5zn9hNJk

該当製品

脆弱性のある製品

公開時点で、この脆弱性は、Cisco Small Businessファームウェアソフトウェアの脆弱性が存在するリリースを実行していて、ACLが設定されたスタック構成の次のシスコ製品に影響を与えました。

- 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
- Business 250 シリーズ スマートスイッチ
- Business 350 シリーズ マネージドスイッチ

ビジネススイッチのスタッカブル構成の詳細については、『シスコビジネススイッチのスタッキングガイドライン』を参照してください。

公開時点で脆弱性が確認されている Cisco ソフトウェアのリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

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。

この脆弱性により、スイッチ上のACL設定が未定義の状態のままになる可能性があります。緩和策として、動作しないVLANからACLのバインドを解除してから、ACLを再度バインドします。これは恒久的な緩和策ではありません。スイッチスタックメンバがリロードされたり、電源が再投入されたりした場合は、再適用する必要があります。

機能していないACLのバインド解除と再バインドの具体的な手順については、『Cisco Business Switches 350 Series CLI Guide』（105 ~ 107ページ）および『Cisco Business 350 Series Switches Administration Guide』（325 ~ 326ページ）を参照してください。詳細なガイダンスが必要な場合は、Cisco Technical Assistance Center(TAC)にお問い合わせください。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

修正済みソフトウェア

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。

修正済みリリース

公開時点では、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

Business 250 シリーズ スマートスイッチおよび Business 350 シリーズ マネージドスイッチ

シスコ ファームウェア リリース	First Fixed Release（修正された最初のリリース）
3.4 以前	3.4.0.17

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、

シスコ ファームウェア リリース	First Fixed Release（修正された最初のリリース）
2.5 以前	2.5.9.54

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、Browse allをクリックし、Switches > LAN Switches - Small Businessの順に選択します。

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、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-bus-acl-bypass-5zn9hNJk

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	2024年1月24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。