Cisco Small Business 100、300、および500シリーズワイヤレスアクセスポイントのコマンドインジェクションとバッファオーバーフローの脆弱性

Medium

アドバイザリーID : cisco-sa-sb-wap-multi-85G83CRB
初公開日 : 2024-03-06 16:00
バージョン 1.0 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwi83952 CSCwi78254 CSCwi83953 CSCwi83951 CSCwi78277 CSCwi83948 CSCwi78271 CSCwi83957

CVE-2024-20335
CVE-2024-20336

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 100、300、および500シリーズワイヤレスアクセスポイント(AP)のWebベースの管理インターフェイスにおける複数の脆弱性により、認証されたリモートの攻撃者が、該当デバイスに対してコマンドインジェクションとバッファオーバーフローの攻撃を実行できる可能性があります。これらの脆弱性を不正利用するには、攻撃者がデバイスの有効な管理者クレデンシャルを持っている必要があります。

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。

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-sb-wap-multi-85G83CRB

該当製品

脆弱性のある製品

公開時点では、これらの脆弱性は、すべてのCisco Small Business 100、300、および500シリーズワイヤレスAPとファームウェアリリースに影響を与えました。

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。

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、他の脆弱性をエクスプロイトする必要はありません。また、いずれかの脆弱性の影響を受ける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-2024-20335:Cisco Small Business 100、300、および500シリーズのワイヤレスAPにおけるコマンドインジェクションの脆弱性

Cisco Small Business 100、300、および500シリーズワイヤレスAPのWebベース管理インターフェイスにおける脆弱性により、認証されたリモートの攻撃者が、該当デバイスに対してコマンドインジェクション攻撃を実行する可能性があります。この脆弱性を不正利用するには、攻撃者がデバイスの有効な管理者クレデンシャルを持っている必要があります。

この脆弱性は、ユーザ指定の入力の検証が不十分であることに起因します。攻撃者は、該当デバイスの Web ベース管理インターフェイスに細工された HTTP リクエスト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。不正利用に成功すると、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として任意のコードを実行する可能性があります。

Bug ID:CSCwi78254、CSCwi78271、CSCwi78277、CSCwi83948
CVE ID：CVE-2024-20335
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.5
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

CVE-2024-20336:Cisco Small Business 100、300、および500シリーズワイヤレスAPのバッファオーバーフローの脆弱性

Cisco Small Business 100、300、および500シリーズワイヤレスAPのWebベースのユーザインターフェイスにおける脆弱性により、認証されたリモートの攻撃者が該当デバイスに対してバッフ

ァオーバーフロー攻撃を実行する可能性があります。この脆弱性を不正利用するには、攻撃者がデバイスの有効な管理者クレデンシャルを持っている必要があります。

この脆弱性は、ユーザ指定の入力の検証が不十分であることに起因します。攻撃者は、該当デバイスの Web ベース管理インターフェイスに細工された HTTP リクエスト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。不正利用に成功すると、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として任意のコードを実行する可能性があります。

Bug ID:CSCwi83951、CSCwi83952、CSCwi83953、CSCwi83957
CVE ID：CVE-2024-20336
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.5
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/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ファームウェアアップデートをリリースしておらず、リリースする予定もありません。Cisco Small Business 100、300、および500シリーズワイヤレスAPは、サポート終了プロセスに入っています。お客様には、これらの製品のサポート終了通知を参照することをお勧めします。

Cisco WAPワイヤレスアクセスポイントの販売終了およびサポート終了のお知らせ

Cisco WAP121 Wireless-Nアクセスポイント（シングルポイント設定）の販売終了およびサポート終了のお知らせ

Cisco WAP371 Wireless-AC/Nアクセスポイント（シングルポイント設定）の販売終了およびサポート終了のお知らせ

Cisco Business Access Pointシリーズへの移行をお勧めします。

デバイスの移行を検討する際は、[シスコ セキュリティ アドバイザリ（Cisco Security Advisories）] 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の有無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。

いずれの場合でも、新しいデバイスがお客様のネットワークニーズに十分対応していること、現在のハードウェアとソフトウェアの構成が新しい製品で引き続き適切にサポートさ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。

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

シスコは、これらの脆弱性を報告していただいたONEKEY Research LabsのQuentin Kaiser氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-multi-85G83CRB

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3月6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。