Cisco Small Business SPA300 シリーズおよび SPA500 シリーズ IP Phone の Web UI の脆弱性

アドバイザリーID : cisco-sa-spa-http-vulns-RJZmX2Xz
初公開日 : 2024-08-07 16:00
バージョン 1.0 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID : CSCwk31988

CVE-2024-20452
CVE-2024-20451
CVE-2024-20454
CVE-2024-20453
CVE-2024-20450

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 SPA300シリーズIPフォンおよびCisco Small Business SPA500シリーズIPフォンのWebベース管理インターフェイスにおける複数の脆弱性により、攻撃者が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したり、サービス妨害(DoS)状態を引き起こしたりする可能性があります。

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。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供していません。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-spa-http-vulns-RJZmX2Xz

該当製品

脆弱性のある製品

これらの脆弱性は、設定に関係なく、Cisco Small Business SPA300シリーズおよびCisco Small Business SPA500シリーズのIPフォンで実行されるすべてのソフトウェアリリースに影

響を与えます。

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。

脆弱性の詳細は以下のとおりです。

CVE-2024-20450、CVE-2024-20452、および CVE-2024-20454：Cisco Small Business SPA300 シリーズおよび SPA500 シリーズ IP Phone の Web UI における任意のコマンド実行の脆弱性

Cisco Small Business SPA300 シリーズ IP Phone および Cisco Small Business SPA500 シリーズ IP Phone の Web ベースの管理インターフェイスに存在する複数の脆弱性により、認証されていないリモート攻撃者が、ルート権限を使用して、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。

これらの脆弱性は、着信 HTTP パケットのエラーが適切にチェックされず、バッファオーバーフローが発生する可能性があるために存在します。攻撃者は、該当デバイスに巧妙に細工された HTTP 要求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、内部バッファをオーバーフローさせ、ルート権限レベルで任意のコマンドを実行する可能性があります。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供していません。これらの脆弱性に対処する回避策はありません。

バグ ID：CSCwk31988
CVE ID：CVE-2024-20450、CVE-2024-20452、および CVE-2024-20454
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：9.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2024-20451 および CVE-2024-20453：Cisco Small Business SPA300 シリーズおよび SPA500 シリーズ IP Phone の Web UI における DoS の脆弱性

Cisco Small Business SPA300 シリーズ IP Phone および Cisco Small Business SPA500 シリーズ IP Phone の Web ベースの管理インターフェイスに存在する複数の脆弱性により、認証されていないリモート攻撃者が、該当デバイスを予期せずリロードさせる可能性があります。

これらの脆弱性は、HTTP パケットのエラーが適切にチェックされないために存在します。攻撃

者は、該当デバイスのリモートインターフェイスに巧妙に細工された HTTP パケッ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。エクスプロイトに成功すると、攻撃者はデバイスで DoS 状態を引き起こす可能性があります。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供していません。これらの脆弱性に対処する回避策はありません。

バグ ID：CSCwk31988
CVE ID：CVE-2024-20451 および CVE-2024-20453
SIR：高
CVSS ベーススコア：7.5
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

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、このアドバイザリで説明している脆弱性に対処するためのソフトウェアの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 SPA300 シリーズ IP Phone および Cisco Small Business SPA500 シリーズ IP Phone 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 IP Phone SPA300 シリーズ（一部のモデル）の販売終了およびサポート終了のお知らせ
- Cisco Small Business SPA303 シリーズ IP Phone の販売終了およびサポート終了のお知らせ
- 他の Cisco Small Business SPA500 シリーズ IP Phone の販売終了およびサポート終了のお知らせ

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、新しい製品タイプ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 BAE Systems Digital Intelligence 社の Aidan 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-http-vulns-RJZmX2Xz

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 8 月 7 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。