Cisco ATA 190シリーズアナログ電話アダプタファームウェアの脆弱性

アドバイザリーID : cisco-sa-ata19x-multi-RDTEqRsy
初公開日 : 2024-10-16 16:00
バージョン 1.0 : Final
CVSSスコア : 8.2
回避策 : No workarounds available
Cisco バグ ID : CSCwf28041 CSCwf28097 CSCwf28191 CSCwf30963 CSCwf28037 CSCwf28048 CSCwf28348 CSCwf28345 CSCwf28378 CSCwf28499 CSCwf28188 CSCwf28398 CSCwf28102 CSCwf28426

CVE-2024-20463
CVE-2024-20462
CVE-2024-20421
CVE-2024-20420
CVE-2024-20458
CVE-2024-20459
CVE-2024-20461
CVE-2024-20460

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 ATA 190シリーズアナログ電話アダプタ(ATA)ファームウェアの複数の脆弱性（オンプレミスとマルチプラットフォームの両方）により、リモート攻撃者が設定の削除や変更、rootユーザとしてのコマンドの実行、インターフェイスのユーザに対するクロスサイトスクリプティング(XSS)攻撃、パスワードの表示、クロスサイトリクエストフォージェリ(CSRF)攻撃、またはデバイスのリブートを実行でき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ファームウェアアップデートをリリースしました。これらの脆弱性に対処する回避策はありません。ただし、Cisco ATA 191オンプレミスファームウェアのみに対して、これらの脆弱性の一部に対処する緩和策があります。

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-ata19x-

multi-RDTEqRsy

該当製品

脆弱性のある製品

これらの脆弱性は、Cisco ATA 190シリーズオンプレミスファームウェアまたはCisco ATA 190シリーズマルチプラットフォームファームウェアの脆弱性が存在するリリースを実行する次のシスコ製品に影響を与えます。

- ATA 191（オンプレミスまたはマルチプラットフォーム）
- ATA 192（マルチプラットフォーム）

脆弱性のある Cisco ファームウェア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。

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。また、これらの脆弱性のいずれかに該当するファームウェアリリースが、他の脆弱性の影響を受けない場合もあります。

脆弱性の詳細は以下のとおりです。

CVE-2024-20458:Cisco ATA 190シリーズアナログ電話アダプタファームウェア認証の脆弱性

Cisco ATA 190シリーズアナログ電話アダプタファームウェアのWebベース管理インターフェイスにおける脆弱性により、認証されていないリモートの攻撃者が該当デバイスの設定を表示または削除したり、ファームウェアを変更したりする可能性があります。

この脆弱性は、特定のHTTPエンドポイントでの認証の欠如に起因します。攻撃者は、特定のURLを参照することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は設定を表示または削除したり、ファームウェアを変更したりできます。

シスコでは、本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います。この脆弱性に対処する回避策はありません。ただし、緩和策があります。手順については、このアドバイザリの「回避策」セクションを参照してください。

バグID: CSCwf28097、CSCwf28102
CVE ID：CVE-2024-20458

セキュリティ影響評価（SIR）：高
CVSS基本スコア：基本8.2
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L

CVE-2024-20421:Cisco ATA 190シリーズアナログ電話アダプタファームウェアのクロスサイトリクエストフォージェリの脆弱性

Cisco ATA 190シリーズアナログ電話アダプタファームウェアのWebベース管理インターフェイスにおける脆弱性により、認証されていないリモートの攻撃者がクロスサイトリクエストフォージェリ(CSRF)攻撃を実行し、該当デバイスで任意のアクションを実行する可能性があります。

この脆弱性は、該当デバイス上の Web ベース管理インターフェイスの CSRF 保護が不十分なことに起因します。攻撃者は、巧妙に細工されたリンクに従うようにユーザを誘導することにより、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、攻撃者はターゲットユーザーの権限を使用して、該当デバイスで任意のアクションを実行できる可能性があります。

シスコでは、本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います。この脆弱性に対処する回避策はありません。ただし、緩和策があります。手順については、このアドバイザリの「回避策」セクションを参照してください。

バグID: CSCwf28426、CSCwf28421
CVE ID：CVE-2024-20421
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.1
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:L

CVE-2024-20459:Cisco ATA 190シリーズアナログ電話アダプタマルチプラットフォームファームウェアのコマンドインジェクションの脆弱性

Cisco ATA 190 マルチプラットフォームシリーズアナログ電話アダプタ(ATA)ファームウェアのWebベース管理インターフェイスにおける脆弱性により、高い権限を持つ認証されたリモートの攻撃者が、基盤となるオペレーティングシステムでrootユーザとして任意のコマンドを実行する可能性があります。

この脆弱性は、Webベースの管理インターフェイスにおける入力サニタイズの欠如に起因します。攻撃者は、Webベースの管理インターフェイスに悪意のある要求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root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できる可能性があります。

シスコでは、本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います。この脆弱性に対処する回避策はありません。ただし、緩和策があります。手順については、このアドバイザリの「回避策」セクションを参照してください。

バグID: CSCwf28499、CSCwf28048
CVE ID：CVE-2024-20459
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-2024-20460:Cisco ATA 190シリーズアナログ電話アダプタファームウェアのリフレクトされたクロスサイトスクリプティングの脆弱性

Cisco ATA 190シリーズアナログ電話アダプタ(ATA)ファームウェアの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、ユーザに対してリフレクトされた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、ユーザ入力の不十分な検証に起因します。攻撃者は、巧妙に細工されたリンクをクリックするようにユーザを誘導することにより、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、攻撃者は影響を受けるインターフェイスに関連する任意のスクリプトコードを実行したり、影響を受けるデバイスのブラウザベースの機密情報にアクセスしたりできる可能性があります。

シスコでは、本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います。この脆弱性に対処する回避策はありません。ただし、緩和策があります。手順については、このアドバイザリの「回避策」セクションを参照してください。

バグID: CSCwf28041、CSCwf28037
CVE ID：CVE-2024-20460
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-2024-20461:Cisco ATA 190シリーズアナログ電話アダプタファームウェアのコマンドインジェクションの脆弱性

Cisco ATA 190シリーズアナログ電話アダプタ(ATA)ファームウェアのCLIの脆弱性により、高い権限を持つ認証されたローカルの攻撃者が、rootユーザとして任意のコマンドを実行できるようになります。

この脆弱性は、CLI入力が適切にサニタイズされていないことに起因しています。攻撃者は、悪意のある文字をCLIに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rootユーザとして基盤となるオペレーティングシステムの読み取りと書き込みを行えるようになります。

シスコでは、本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: CSCwf28378、CSCwf30963
CVE ID：CVE-2024-20461
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.0
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

CVE-2024-20462:Cisco ATA 190シリーズアナログ電話アダプタマルチプラットフォームファームウェアの情報開示の脆弱性

Cisco ATA 190シリーズマルチプラットフォームアナログ電話アダプタファームウェアのWebベース管理インターフェイスにおける脆弱性により、権限の低い認証されたローカルの攻撃者が、該当デバイスのパスワードを表示できるようになります。

この脆弱性は、該当デバイスからのHTMLコンテンツの不適切なサニタイズに起因します。エクスプロイトに成功すると、攻撃者は他のユーザに属するパスワードを表示できる可能性があります。

シスコでは、本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:CSCwf28398
CVE ID：CVE-2024-20462
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.5
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVE-2024-20463:Cisco ATA 190シリーズアナログ電話アダプタファームウェアのコマンドインジェクションおよびDoS脆弱性

Cisco ATA 190シリーズアナログ電話アダプタファームウェアのWebベース管理インターフェイスにおける脆弱性により、認証されていないリモートの攻撃者が設定を変更したり、該当デバイスをリブートしたりする可能性があります。

この脆弱性は、HTTPサーバがGET要求の状態変更を許可してい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悪意のある要求を送信することで、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、攻撃者は設定を限定的に変更したり、デバイスをリブートしたりして、サービス妨害(DoS)状態を引き起こす可能性があります。

シスコでは、本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います。この脆弱性に対処する回避策はありません。ただし、緩和策があります。手順については、このアドバイザリの「回避策」セクションを参照してください。

バグID: CSCwf28345、CSCwf28348

CVE ID：CVE-2024-20463
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.4
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L

CVE-2024-20420:Cisco ATA 190シリーズアナログ電話アダプタファームウェアの特権昇格の脆弱性

Cisco ATA 190シリーズアナログ電話アダプタファームウェアのWebベース管理インターフェイスにおける脆弱性により、権限の低い認証されたリモートの攻撃者が管理者ユーザとしてコマンドを実行できる可能性があります。

この脆弱性は、HTTPサーバによる不正な認証検証に起因します。攻撃者は、Webベースの管理インターフェイスに悪意のある要求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、攻撃者は管理者ユーザとしてコマンドを実行できる可能性があります。

シスコでは、本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います。この脆弱性に対処する回避策はありません。ただし、緩和策があります。手順については、このアドバイザリの「回避策」セクションを参照してください。

バグID: CSCwf28191、CSCwf28188
CVE ID：CVE-2024-20420
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.4
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/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。ただし、次の脆弱性に対してのみ緩和策があります。

CVE-2024-20458、CVE-2024-20421、CVE-2024-20459、CVE-2024-20460、CVE-2024-20463、CVE-2024-20420

Webベースの管理インターフェイスは、Cisco ATA 191オンプレミスファームウェアで無効にすることができます。デフォルトでディセーブルになっている。詳細については、『Cisco Unified Communications Managerセキュリティガイド』を参照してください。

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

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。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

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。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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

次の表に示すように、該当する修正済みのソフトウェアリリースにアップグレードすることをお勧めします。

Cisco IP Phone モデル	Cisco Bug ID		脆弱性のあるリリース	First Fixed Release（修正された最初のリリース）
ATA 191 Analog Telephone Adapter	CSCwf28102 CSCwf28041 CSCwf28378	CSCwf28348 CSCwf28191 CSCwf28426	12.0.1 以前	12.0.2
ATA 191および192マルチプラットフォームアナログ電話アダプタ	CSCwf28097 CSCwf28499 CSCwf28048 CSCwf28037 CSCwf30963	CSCwf28398 CSCwf28345 CSCwf28188 CSCwf28421	11.2.4 以前	11.2.5

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とその公表は確認しておりません。

出典

これらの脆弱性は、内部セキュリティテストの実施中に、Cisco Advanced Security Initiatives Group（ASIG）の Zack Sanchez によって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multi-RDTEqRsy

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10月16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、単独の転載や意訳を施した場合、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。