Cisco ATA 190 シリーズ アナログ電話アダプタ ソフトウェアの脆弱性

Medium

アドバイザリーID : cisco-sa-ata19x-multivuln-GEZYVvs
初公開日 : 2022-10-05 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : No workarounds available
Cisco バグ ID : CSCwa24837 CSCwa24849 CSCwa24844 CSCvz91984 CSCvz93504 CSCwa24842 CSCvz93493

CVE-2022-20689
CVE-2022-20766
CVE-2022-20688
CVE-2022-20687
CVE-2022-20686
CVE-2022-20691
CVE-2022-20690

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ソフトウェアのCisco Discovery Protocol(CDP)およびLink Layer Discovery Protocol(LLDP)の複数の脆弱性により、攻撃者がコードを実行したり、サービスの予期せぬリロードを引き起こしたり、該当デバイスでCisco Discovery ProtocolまたはLLDPデータベースを破損させたりする可能性があります。

注：Cisco Discovery ProtocolとLLDPはレイヤ2プロトコルです。これらの脆弱性をエクスプロイトするには、攻撃者は該当デバイスと同じブロードキャストドメイン内に存在する（レイヤ 2 と隣接関係にある）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。

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-ata19x-

multivuln-GEZYVvs

該当製品

脆弱性のある製品

公開時点で、これらの脆弱性は、Cisco ATA 190シリーズオンプレミスソフトウェアまたはCisco ATA 190シリーズマルチプラットフォーム(MPP)ソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えました。

- ATA 190（オンプレミスのみ）
- 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のみ）

脆弱性が存在するCiscoソフト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、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-2022-20686、CVE-2022-20687:Cisco ATA 190シリーズアナログ電話アダプタリンクレイヤ検出プロトコルファームウェアの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Link Layer Discovery Protocol(LLDP)機能における複数の脆弱性により、認証されていないリモートの攻撃者が該当デバイスで任意のコードを実行し、LLDPサービスを再起動できる可能性があります。

これらの脆弱性は、特定のLLDPパケットヘッダーフィールドの長さ検証が欠落していることに起因します。攻撃者は、該当デバイスに悪意のあるLLDPパケットを送信することで、これら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、攻撃者は該当デバイスでコードを実行し、LLDPを予期せず再起動させ、サービス拒否(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。

バグID:CSCvz93493、CSCvz91984、CSCvz93504
CVE ID:CVE-2022-20686、CVE-2022-20687
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.3
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVE-2022-20688:Cisco ATA 190シリーズアナログ電話アダプタのCisco Discovery Protocolファームウェアにおける 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Cisco Discovery Protocol機能の脆弱性により、認証されていないリモートの攻撃者が該当デバイスで任意のコードを実行し、Cisco Discovery Protocolサービスを再起動できる可能性があります。

この脆弱性は、特定のCisco Discovery Protocolパケットヘッダーフィールドの長さ検証が欠落していることに起因します。攻撃者は、該当デバイスに悪意のあるCisco Discovery Protocolパケットを送信することにより、これら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、攻撃者は該当デバイスでコードを実行し、Cisco Discovery Protocolを予期せず再起動させ、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。

バグID:CSCvz93493、CSCvz91984、CSCvz93504
CVE ID：CVE-2022-20688
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.3
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVE-2022-20689、CVE-2022-20690:Cisco ATA 190シリーズアナログ電話アダプタのCisco Discovery Protocolファームウェア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ファームウェアのCisco Discovery Protocol機能における複数の脆弱性により、認証されていない隣接する攻撃者が該当デバイスでCisco Discovery Protocolのメモリ破損を引き起こす可能性があります。

これらの脆弱性は、Cisco Discovery Protocolメッセージを処理する際の長さ検証チェックがないことに起因します。攻撃者は、該当デバイスに悪意のあるCisco Discovery Protocolパケットを送信することにより、これら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、有効なCisco Discovery Protocolパケットデータの範囲外の読み取りが引き起こされ、影響を受けるデバイスの内部Cisco Discovery Protocolデータベースが破損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。

バグID:CSCvz93493、CSCvz91984、CSCvz93504
CVE ID:CVE-2022-20689、CVE-2022-20690
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.3
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVE-2022-20691: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Cisco Discovery ProtocolにおけるDoS脆弱性

Cisco ATA 190シリーズ適応型電話アダプタファームウェアのCisco Discovery Protocol機能の脆弱性により、認証されていない隣接する攻撃者が該当デバイスにDoS状態を引き起こす可能性があります。

この脆弱性は、特定のCisco Discovery Protocolパケットヘッダーフィールドの長さ検証が欠落していることに起因します。攻撃者は、巧妙に細工されたCisco Discovery Protocolパケットを該当デバイス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、攻撃者はデバイスの使用可能なメモリを枯渇させ、サービスを再起動させ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:CSCwa24837,CSCwa24842
CVE ID：CVE-2022-20691
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.3
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVE-2022-20766: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Cisco Discovery ProtocolにおけるDoS脆弱性

Cisco ATA 190シリーズ適応型電話アダプタファームウェアのCisco Discovery Protocol機能の脆弱性により、認証されていないリモート攻撃者が該当デバイスにDoS状態を引き起こす可能性があります。

この脆弱性は、Cisco Discovery Protocolパケットを処理する際の範囲外の読み取りに起因します。攻撃者は、巧妙に細工されたCisco Discovery Protocolパケットを該当デバイス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、攻撃者はサービスを再起動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。

Bug ID:CSCwa24844、CSCwa24849

CVE ID：CVE-2022-20766
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.3
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

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、管理者は影響を受ける機能を無効にすることができます。

デバイスのLANインターフェイスでCisco Discovery ProtocolまたはLLDPを無効にするには、Web UIを開き、Network Setup > Advanced Settings > CDP &LLDPの順に選択します。次に、Enabled CDPまたはEnabled LLDPのチェックマークを外します。

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

発行時点では、次の表に記載されている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。

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 190 アナログ電話アダプタ	CSCvz93493、CSCvz91984、CSCvz93504、CSCwa24837、CSCwa24849	ソフトウェアメンテナンスは終了しました。公開済みの修正プログラムはありません.次の項を参照してください。	

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	CSCvz93493、CSCvz91984、CSCvz93504、CSCwa24837、CSCwa24849	12.0(1)SR4以前	12.0(1)SR5
ATA 191 マルチプラットフォーム アナログ電話アダプタ	CSCvz93493、CSCvz91984、CSCvz93504、CSCwa24842、CSCwa24844	11.2.1 以前	11.2.2
ATA 192 マルチプラットフォーム アナログ電話アダプタ	CSCvz93493、CSCvz91984、CSCvz93504、CSCwa24837、CSCwa24849	11.2.1 以前	11.2.2

Cisco ATA 190 Analog Telephone Adapter(ATA)(CSCvz93493、CSCvz91984、CSCvz93504、CSCwa24837、CSCwa24849)

シスコでは、Cisco ATA 190 Analog Telephone Adapterに関するこの脆弱性に対処するソフトウェアアップデートのリリースとリリースを行っていません。これは、この製品がサポート終了のプロセスに入ったためです。製品のサポート終了のお知らせを参照することをお勧めします。

Cisco ATA 190 アナログ電話アダプタ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。

いずれの場合も、新しいデバイスがネットワークのニーズに十分であること、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しい製品で引き続き適切にサポートされていることを確認する必要があります。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。

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

シスコは、これらの脆弱性を報告してくださった、Qi'anxin Group、Legendsec の Codesafe チームの Qian Chen 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs

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	2022 年 10 月 5 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。