マルチプラットフォーム ファームウェア搭載の Cisco IP Phone 6800、7800、および 8800 シリーズの脆弱性

High

アドバイザリーID : cisco-sa-ipphone-multi-vulns-cXAhCvS
初公開日 : 2024-05-01 16:00
バージョン 1.0 : Final
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco バグ ID : CSCwi64064 CSCwi64050 CSCwi64077 CSCwi64037 CSCwi64103 CSCwi64082

CVE-2024-20376
CVE-2024-20357
CVE-2024-20378

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 IP Phoneファームウェアの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サービス拒否(DoS)状態を引き起こしたり、不正アクセスを受けたり、該当システムの機密情報を参照したり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-ipphone-multi-vulns-cXAhCvS

該当製品

脆弱性のある製品

これらの脆弱性は、Cisco IP Phone ファームウェアの脆弱性が存在するリリースを実行している次のシスコ製品に影響を与えます。

- IP Phone 6800 シリーズ マルチプラットフォーム ファームウェア
- IP Phone 7800 シリーズ マルチプラットフォーム ファームウェア
- IP Phone 8800 シリーズ マルチプラットフォーム ファームウェア
- マルチプラットフォーム モードの Video Phone 8875

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、これらの脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- ATA 191 Analog Telephone Adapter
- IP Conference Phone 7832
- IP Conference Phone 8832
- IP 電話 7800 シリーズ
- IP 電話 8800 シリーズ
- IP Phone 8845 および 8865
- Unified IP Phone 3905
- Unified IP 電話 6901 および 6911
- Video Phone 8875
- Webex Room Phone
- Webex Share
- Webex Wireless Phone 840 および 860
- ワイヤレス IP Phone 8821

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。さらに、いずれかの脆弱性の影響を受けるソフトウェア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-2024-20376：Cisco IP Phone のサービス妨害（DoS）の脆弱性

Cisco IP Phone 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影響を受けるデバイスをリロードさせ、サービス妨害（DoS）状態を発生させる可能性があります。

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巧妙に細工された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。エクスプロイトに成功した場合、攻撃者は脆弱性の影響を受けるデバイスをリロードさせることができます。

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。

バグ ID：CSCwi64103、CSCwi64077
CVE ID：CVE-2024-20376
セキュリティ影響評価（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

CVE-2024-20378：Cisco IP Phone の情報開示の脆弱性

Cisco IP Phone 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影響を受けるデバイスから機密情報を取得する可能性があります。

この脆弱性は、影響を受けるデバイス上の Web ベース管理インターフェイスにおける特定のエンドポイントに対する認証が不足していることに起因しています。攻撃者は、影響を受けるデバイスに接続することで、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、攻撃者はデバイスへの不正アクセスを取得し、影響を受けるデバイスとの間で送受信されるユーザーログイン情報とトラフィック（再生可能な VoIP コールを含む）を記録する可能性があります。

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。

バグ ID：CSCwi64037、CSCwi64050
CVE ID：CVE-2024-20378
セキュリティ影響評価（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:H/I:N/A:N

CVE-2024-20357：Cisco IP Phone の不正アクセスの脆弱性

Cisco IP Phone ファームウェアの XML サービスの脆弱性により、認証されていないリモートの攻撃者が影響を受けるデバイスで通話を開始する可能性があります。

この脆弱性は、XML リクエストの解析中に境界チェックが実行されないために発生します。攻撃者は、細工された XML リクエストを影響を受けるデバイスに送信することで、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、攻撃者はデバイスで通話を開始したり、音声を再生したりする可能性があります。

注：XML サービスはデフォルトで無効になっています。

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。

バグ ID：CSCwi64082、CSCwi64064
CVE ID：CVE-2024-20357
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

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

次の表では、左の列にシスコソフトウェアのリリースを記載しています。右の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこれらの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な修正済み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。

IP Phone 6800、7800、および 8800 マルチプラットフォーム ファームウェア

Cisco マルチプラットフォーム 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）
12.0.4 以前	12.0.4SR1

Video Phone 8875

Cisco PhoneOS のリリース	First Fixed Release（修正された最初のリリース）
2.3.1.001 以前	2.3.1.0101

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

シスコは、これらの脆弱性を報告していただいた Mantra Information Security の Balazs Bucsay

氏、Davinsi Labs の Peter Lemmens 氏と Liviu Rombaut 氏、および Cyberwisec の Andras Kosztyu 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-multi-vulns-cXAhCvS

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 5 月 1 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。