

Cisco IP Phone 6800、7800、および8800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



アドバイザーID : cisco-sa-ipphone-multi- [CVE-2024-20376](#)
vulns-cXAhCvS
初公開日 : 2024-05-01 16:00 [CVE-2024-20357](#)
バージョン 1.0 : Final [CVE-2024-20378](#)
CVSSスコア : [7.5](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCwi64064](#) [CSCwi64050](#)
[CSCwi64077](#) [CSCwi64037](#) [CSCwi64103](#)
[CSCwi64082](#)

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ーの「[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。

このアドバイザーは、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
- Video Phone 8875 マルチプラットフォームモード

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DoS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リロードを引き起こし、その結果、DoS状態が発生す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の情報漏えいの脆弱性

Cisco IP PhoneファームウェアのWebベースの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、該当デバイスのWebベース管理インターフェイスの特定のエンドポイントに対する認証が行われないことに起因します。攻撃者は、該当デバイスに接続することで、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、攻撃者はデバイスへの不正アクセスを許可され、リプレイ可能なVoIPコールを含む、影響を受けるデバイスとの間のユーザクレデンシャルとトラフィックの記録が可能になります。

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該当デバイスで通話を開始できる可能性があります。

この脆弱性は、XML要求の解析中に境界チェックが行われないために存在します。攻撃者は、巧妙に細工されたXML要求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、攻撃者はコールを開始したり、デバイスで音声を再生したりできます。

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ン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です。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社のBalazs

Bucsay氏、Davinsi Labs社のPeter Lemmens氏、Davinsi Labs社のLiviu Rombaut氏、Cyberwisec社のAndras Kosztyu氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iphone-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

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、単独の転載や意識を施した場合、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。