

# Cisco 7800、8800、および9800シリーズ電話機の情報漏えいの脆弱性



アドバイザリーID : cisco-sa-phone-infodisc-sbyqQVbG

[CVE-2024-20445](#)

初公開日 : 2024-11-06 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 : [CSCwk32410](#) [CSCwk25862](#)

[CSCwk25863](#) [CSCwk25869](#)

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 Desk Phone 9800シリーズ、Cisco IP Phone 7800および8800シリーズ、Cisco Video Phone 8875のWeb UI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の機密情報にアクセスする可能性があります。

この脆弱性は、Session Initiation Protocol(SIP)ベースの電話ロードのWeb UI内での機密情報の不適切な保存に起因します。攻撃者は、Webアクセスが有効になっているデバイスのIPアドレスを参照することで、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、攻撃者は着信および発信コールレコードなどの機密情報にアクセスできる可能性があります。

注 : Web Access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。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-phone-infodisc-sbyqQVbG>

## 該当製品

### 脆弱性のある製品

公開時点では、この脆弱性は、Cisco SIP IP Phoneソフトウェアの脆弱性のあるリリースを実行し、Webアクセスを有効にしている次のシスコ製品に影響を与えました。

- Desk Phone 9800シリーズ
- IP 電話 7800 シリーズ
- IP Phone 8800シリーズ ( Cisco Wireless IP Phone 8821を除く )
- Video Phone 8875

Webアクセス機能は、デフォルトでは無効になっています。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。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。

## Webアクセスが有効になっているかどうかの確認

Webアクセスは、シスコの電話機ではデフォルトで無効になっています。ユーザが次の手順に従って、電話機の設定にリストされているIPアドレスを参照できる場合、Webアクセスは有効になっています。

1. 電話機の前面にある歯車アイコンを選択して電話機の設定にアクセスし、電話機のIPアドレスを確認します。
2. Admin settings > Network Setup > Ethernet setupまたはWi-Fi client setup > IPv4 setupの順に選択します。
3. ブラウザウィンドウでIPアドレスを入力し、Enterキーを押します。

Device Information画面が表示されている場合は、電話機でWeb Accessが有効になっています。

Web Accessを有効または無効にするには、次の手順を実行します。

1. 管理者権限を使用して、電話機が登録されているCommunications Managerにログインします。管理者権限を使用すると、デバイスを変更できます。
2. [Device] > [Phone] を選択します。
3. 検索条件を入力して、Findを選択します。
4. Device Nameリストから適切なデバイスを選択します。
5. Web Accessまでスクロールダウンし、必要に応じてEnabledまたはDisabledを切り替えて、Saveをクリックします。
6. ブラウザウィンドウにIPアドレスを入力し、Enterキーを押して、目的の状態が設定されていることを確認します。

## 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、この脆弱性の影響を受けることが分かっています。](#)

シスコでは、この脆弱性がCiscoマルチプラットフォームファームウェアを実行しているCisco IP Phone 7800シリーズまたは8800シリーズの電話機には影響を与えないことを確認しました。

## 回避策

こ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

[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

このドキュメントの発行時点では、次の表に示す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。

左側の列にはシスコソフトウェアリリース、右側の列に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、およびこの脆弱性に対する修正を含むリリースが示されています。

### Desk Phone 9800シリーズ

Cisco SIP IP Phoneソフトウェアリリース	First Fixed Release ( 修正された最初のリリース )
3.1(1)	3.2(1)
3.1(1)SR1	3.2(1)

### IP Phone 7800および8800シリーズ

Cisco SIP IP Phoneソフトウェアリリース	First Fixed Release ( 修正された最初のリリース )
14.3 より前	修正済みリリースに移行。
14.3	14.3(1)

### Video Phone 8875

Cisco SIP IP Phoneソフトウェアリリース	First Fixed Release ( 修正された最初のリリース )
2.3(1)SR1以前	修正済みリリースに移行。
3.2(1)	脆弱性なし

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、この脆弱性を報告していただいたSecunnixのBekir KAYA氏に感謝いたします。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-phone-infodisc-sbyqQVbG>

## 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11月6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。