Cisco Desk Phone 9800シリーズ、IP Phone 7800および8800シリーズ、およびSIPソフトウェアの脆弱性が存在するVideo Phone 8875

Medium

アドバイザリーID : cisco-sa-phone-write-g3kcC5Df
初公開日 : 2025-09-03 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 : CSCwn52913 CSCwn51679 CSCwn51677 CSCwn55709 CSCwn52920 CSCwn55726 CSCwn52910 CSCwn52921 CSCwn55714 CSCwn55725 CSCwn52911 CSCwn52922 CSCwn55728 CSCwn55727 CSCwn52919 CSCwn52909 CSCwn55710 CSCwn55712

CVE-2025-20335
CVE-2025-20336

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 Session Initiation Protocol(SIP)ソフトウェアを搭載したCisco Video Phone 8875のディレクトリアクセス許可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に対して任意のファイル書き込みと情報漏えいの攻撃を実行できる可能性があります。

注：これらの脆弱性を不正利用するには、電話でWebアクセスを有効にする必要があります。Web アクセスはデフォルトで無効になっています。

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-phone-

write-g3kcC5Df

該当製品

脆弱性のある製品

公開時点で、Cisco SIP 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が、この脆弱性の影響を受けました。

- Desk Phone 9800シリーズ
- IP 電話 7800 シリーズ
- IP 電話 8800 シリーズ
- 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。

このアドバイザリの公開時点で脆弱性が存在するシスコ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。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、電話機の設定に表示されているIPアドレスを参照できる場合は、Webアクセスが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にIPアドレスを入力し、Enterをクリックします。

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

Webアクセス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. 検索基準を入力し、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。

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、いずれかの脆弱性の影響を受ける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-2025-20335:Cisco Desk Phone 9800シリーズ、IP Phone 7800および8800シリーズ、Video Phone 8875（SIPソフトウェア搭載）における任意のファイル書き込みの脆弱性

Cisco Desk Phone 9800シリーズ、Cisco IP Phone 7800および8800シリーズ、Cisco Video Phone 8875のディレクトリアクセス許可の脆弱性により、認証されていないリモートの攻撃者が該当デバイスに任意のファイルを書き込む可能性があります。

この脆弱性は、適切な認証制御がないことに起因します。細工された要求が該当デバイスに送信されると、この脆弱性がエクスプロイトされる危険性があります。エクスプロイトに成功すると、攻撃者は基盤となるオペレーティングシステムの特定のディレクトリに対して任意のファイル書き込みを実行できる可能性があります。

注：この脆弱性を不正利用するには、電話でWebアクセスが有効になっている必要があります。Web アクセ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: CSCwn51679、CSCwn55709、CSCwn55710、CSCwn55710 2、CSCwn55714、CSCwn55725、CSCwn55726、CSCwn55727、CSCwn55728
CVE ID：CVE-2025-20335
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-2025-20336:Cisco Desk Phone 9800シリーズ、IP Phone 7800および8800シリーズ、およびSIPソフトウェア情報漏えい機能付きVideo Phone 8875の脆弱性

Cisco Desk Phone 9800シリーズ、Cisco IP Phone 7800および8800シリーズ、Cisco Video Phone 8875のディレクトリアクセス許可の脆弱性により、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できる可能性があります。

この脆弱性は、機密情報へのアクセスを明示的に許可されていないアクターに機密情報が公開されるために存在します。攻撃者は、Webアクセスが有効になっているデバイスのIPアドレスに巧妙に細工されたパケットを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、攻撃者はデバイスから機密情報にアクセスできる可能性があります。

注：この脆弱性を不正利用するには、電話でWebアクセスが有効になっている必要があります。Web アクセ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: CSCwn51677、CSCwn52909、CSCwn52910、CSCwn52910 1、CSCwn52913、CSCwn52919、CSCwn52920、CSCwn52921、CSCwn52922
CVE ID：CVE-2025-20336
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:L/I:N/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

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、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

公開時点では、次の表の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。

左の列にはシスコソフトウェアリリースが、右の列にはリリースがこのアドバイザリに記載された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リリースが示されています。

Desk Phone 9800シリーズ

Cisco SIP 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	3.3(1)

IP Phone 7800および8800シリーズ

Cisco SIP 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)SR2

IP Phone 8821

Cisco SIP 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）
11 より前	修正済みリリースに移行。
11	11.0(6)SR7

Video Phone 8875

Cisco SIP 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	3.3(1)

シスコの 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済み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

CVE-2025-20335：この脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のKent Yoderによる内部セキュリティテストで発見されました。

CVE-2025-20336：この脆弱性は、Cisco ASIGのZach Sanchezによる内部セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-phone-write-g3kcC5Df

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	2025年9月3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。