

Cisco Desk Phone 9800シリーズ、IP Phone 7800および8800シリーズ、およびSIPソフトウェアを搭載したVideo Phone 8875のサービス妨害の脆弱性



アドバイザリーID : cisco-sa-phone-dos-txMYNRzv

[CVE-2026-20281](#)

初公開日 : 2026-09-02 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 : [CSCwu46391](#) [CSCwu46407](#)

[CSCwu46394](#) [CSCwu46395](#) [CSCwu46397](#)

[CSCwu46389](#) [CSCwu56541](#) [CSCwu69663](#)

[CSCwu46404](#) [CSCwu46406](#)

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 Session Initiation Protocol(SIP)ソフトウェアを実行する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サービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、該当デバイスがHTTPパケットを処理する際の不適切なメモリ管理に起因します。攻撃者は、巧妙に細工されたHTTPパケットの連続的なストリームを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、攻撃者は該当デバイスでメモリを継続的に消費させ、その結果DoS状態が発生する可能性があります。この状態から回復するには、デバイスを手動で再起動する必要があります。

注 : この脆弱性を悪用するには、電話機をCisco Unified Communications Manager(Unified CM)に登録し、Web Access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。

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-dos-txMYNRzv>

該当製品

脆弱性のある製品

この脆弱性は、Cisco SIPソフトウェアの脆弱性のあるリリースを実行し、Cisco Unified CMに登録され、Web Accessを有効にしている次のシスコ製品に影響を与えます。

- 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。

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。

Web アクセスが有効になっているかどうかの確認

Web アクセスが有効になっているかどうかを確認するには、次の手順を実行します。

1. 電話機の前面にある歯車アイコンを押して、[設定 (Settings)] メニューにアクセスします。
2. Admin settings > Network Setup > Ethernet setupまたはWi-Fi client setup > IPv4 setupの順に選択します。電話機の IP アドレスを確認します。
3. インターネットにアクセスできるデバイスで Web ブラウザを開き、IP アドレスをアドレスバーに入力します。Enter を押します。

Web ブラウザに [デバイス情報 (Device Information)] 画面が表示される場合は、電話機で Web アクセスが有効になっています。

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](#)にリストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコでは、これらの脆弱性が、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 シリーズには影響を及ぼさないことを確認しています。

回避策

この脆弱性に対処する回避策はありません。ただし、Web Accessを無効にすることで、この脆弱性は軽減されます。

特定のデバイスでWebアクセスを無効にするには、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Unified CM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. 検索ボックスに検索条件を入力し、[検索 (Find)] をクリックします。
4. [デバイス名 (Device Name)] リストから適切なデバイスを選択します。
5. Web Accessでトグルボタンを使用してDisabledを選択します。
6. [Save] をクリックします。

Webアクセスが無効になっていることを確認するには、インターネットアクセスを使用するデバイスのブラウザウィンドウで電話機のIPアドレスを入力し、Enterをクリックします。IPアドレスに到達できない場合、Webアクセスは無効になっています。

複数のデバイスでWebアクセスを無効にするには、『[Bulk Administration Guide for Cisco Unified Communications Manager](#)』の説明に従ってBulk Admin Tool(BAT)を使用します。

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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

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。右側の列は、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。

Desk Phone 9800シリーズおよび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)
4.1(1)SR1以前	修正済みリリースに移行。
5	5.0(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)
14.4 より前	修正済みリリースに移行。
14.4	14.4(1)SR3

IP Phone 8845 および 8865

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)
14.4 より前	修正済みリリースに移行。
14.4	14.4(1)SR4

ワイヤレス 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)
11.0 より前	修正済みリリースに移行。
11.0	11.0(6)SR8

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

シスコは、この脆弱性を報告していただいたBertie Hallows氏に感謝いたします。

URL

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

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	2026年9月2日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。