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

High

アドバイザリーID : cisco-sa-phone-dos-FPyjLV7A
初公開日 : 2025-10-15 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 : CSCwn51601 CSCwn60481 CSCwn60492 CSCwn60480 CSCwn60491 CSCwn60494 CSCwn60482 CSCwn60493 CSCwn60484 CSCwn58674 CSCwn58685 CSCwn58673 CSCwn58684 CSCwn58683 CSCwn58671 CSCwn51683 CSCwn58676 CSCwn58687

CVE-2025-20350
CVE-2025-20351

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している Cisco Desk Phone 9800 シリーズ、Cisco IP Phone 7800 および 8800 シリーズ、および Cisco Video Phone 8875 の複数の脆弱性により、認証されていないリモート攻撃者がサービス妨害（DoS）状態を引き起こしたり、Web UI のユーザーに対してクロスサイト スクリプティング（XSS）攻撃を実行したりする可能性があります。

注：これらの脆弱性を エクスプロイトするには、電話機を Cisco Unified Communications Manager に登録し、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-dos-FPyjLV7A

該当製品

脆弱性のある製品

これらの脆弱性の影響を受けるのは、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 Communications Manager に登録され、Web アクセスが有効になっている次のシスコ製品です。

- 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。

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。

Cisco Desk Phone 9800 シリーズ、IP Phone 7800 および 8800 シリーズ、Video Phone 8875 の SIP ソフトウェアにおける DoS の脆弱性

Cisco SIP ソフトウェアを実行している 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 Web UI に存在する脆弱性により、認証されていないリモート攻撃者が該当デバイスで 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バッファオーバーフローに起因します。攻撃者は、巧妙に細工された HTTP 入力をデバイスに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。不正利用に成功すると、攻撃者は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。

注：この脆弱性をエクスプロイトするには、電話機を Cisco Unified Communications Manager に登録し、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。

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: CSCwn51601、CSCwn60480、CSCwn60481、CSCwn60488 2、CSCwn60484、CSCwn60491、CSCwn60492、CSCwn60493、CSCwn60494
CVE ID：CVE-2025-20350
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

Cisco Desk Phone 9800 シリーズ、IP Phone 7800 および 8800 シリーズ、Video Phone 8875 の SIP ソフトウェアにおける XSS の脆弱性

Cisco SIP ソフトウェアを実行している 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 Web UI に存在する脆弱性により、認証されていないリモート攻撃者が Web UI のユーザーに対して XSS 攻撃を実行する可能性があります。

この脆弱性は、該当デバイスの Web UI でユーザー入力が十分に検証されないことに起因します。攻撃者は、ユーザーを、巧妙に細工されたリンクをクリックするように誘導することで、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、攻撃者は該当イ

ンターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセスする可能性があります。

注：この脆弱性をエクスプロイトするには、電話機を Cisco Unified Communications Manager に登録し、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。

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: CSCwn51683、CSCwn58671、CSCwn58673、CSCwn58677 4、CSCwn58676、CSCwn58683、CSCwn58684、CSCwn58685、CSCwn58687
CVE ID：CVE-2025-20351
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.1
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/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。ただし、Web アクセスを無効にすることで、これら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アクセス（Web Access）] で、トグルボタンを使用して [有効（Enabled）] または [無効（Disabled）] を選択し、[保存（Save）] をクリックします。

目的の状態が設定されたことを確認するには、インターネットにアクセスできるデバイスのブラウザウィンドウに電話機の IP アドレスを入力し、[Enter] をクリックします。

複数のデバイスで Web アクセスを有効または無効にするには、『Cisco Unified Communications Manager 一括管理ガイド』に記載されている一括管理ツール（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。これら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。中央および右の列は、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。

Desk Phone 9800 シリーズ

Cisco SIP ソフトウェアリリース	CVE-2025-20350 の最初の修正済みリリース	CVE-2025-20351 の最初の修正済みリリース
3	3.3(1)	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	CVE-2025-20350 の最初の修正済みリリース	CVE-2025-20351 の最初の修正済みリリース
14.3 より前	修正済みリリースに移行。	修正済みリリースに移行。
14.3	14.3(1)SR2	修正済みリリースに移行。
14.4	脆弱性なし	14.4(1)

IP Phone 8821

Cisco SIP ソフトウェアリリース	CVE-2025-20350 の最初の修正済みリリース	CVE-2025-20351 の最初の修正済みリリース
11 より前	修正済みリリースに移行。	修正済みリリースに移行。
11	11.0(6)SR7	11.0(6)SR7

Video Phone 8875

Cisco SIP ソフトウェアリリース	CVE-2025-20350 の最初の修正済みリリース	CVE-2025-20351 の最初の修正済みリリース
2.3(1)SR1 以前	修正済みリリースに移行。	修正済みリリースに移行。
3	3.3(1)	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とその公表は確認しておりません。

出典

これらの脆弱性は、内部セキュリティテストの実施中に、Cisco Advanced Security Initiatives Group（ASIG）の Kent Yoder によって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-phone-dos-FPyjLV7A

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 10 月 15 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。