Cisco IP Phoneに保存されたクロスサイトスクリプティングの脆弱性

アドバイザリーID : cisco-sa-uipphone-xss-NcmUykqA
CVE-2023-20265
初公開日 : 2023-11-15 16:00
バージョン 1.0 : Final
CVSSスコア : 5.5
回避策 : No workarounds available
Cisco バグ ID : CSCwf58578 CSCwf58592 CSCwf58594

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の小さなサブセットにおけるWebベースの管理インターフェイスの脆弱性により、認証されたリモートの攻撃者が、該当デバイスのインターフェイスのユーザに対してストアドクロスサイトスクリプティング(XSS)攻撃を実行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、悪意のあるHTMLまたはスクリプトコンテンツを含むページを表示するよう該当インターフェイスのユーザを誘導することで、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。この脆弱性を不正利用するには、攻撃者が該当デバイスのWebベース管理インターフェイスにアクセスするための有効なクレデンシャルを持っている必要があります。

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。

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-uipphone-xss-NcmUykqA

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 IP Phoneソフトウェアの脆弱性のあるリリースを実行している次のシスコ製品に影響を与えました。

- IP DECT 110マルチプラットフォームファームウェア搭載シングルセルベースステーション(CSCwf58578)
- IP DECT 210マルチセルベースステーションマルチプラットフォームファームウェア(CSCwf58578)
- Unified IP Phone 6901(CSCwf58592)
- Unified SIP Phone 3905(CSCwf58594)

注：電話機のデフォルト設定は、この脆弱性の影響を受けます。

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。

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 190 シリーズ アナログ電話アダプタ
- ATA 191アナログ電話アダプタ
- ATA 192マルチプラットフォームアナログ電話アダプタ
- IP DECT 6823 マルチプラットフォーム ファームウェア
- IP DECT 6825 マルチプラットフォーム ファームウェア
- IP Conference Phone 7832
- IP Conference Phone 7832 マルチプラットフォーム ファームウェア
- IP Conference Phone 8832
- IP Conference Phone 8832 マルチプラットフォーム ファームウェア
- IP 電話 7800 シリーズ
- IP 電話 8800 シリーズ
- 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
- Unified IP Phone 7900 シリーズ
- Unified IP Conference Phone 8831
- サードパーティコール制御向け Unified IP Conference Phone 8831
- Video Phone 8875
- Webex会議室の電話
- Webex Share

- Webex Wireless Phone 840 および 860
- ワイヤレス IP Phone 8821

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

公開時点では、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。

IP DECT 110シングルセル基地局（マルチプラットフォームファームウェア搭載）またはIP DECT 210マルチセル基地局（マルチプラットフォームファームウェア搭載）

Cisco IP Phone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）
5.1.1 以前	修正済みリリースに移行。
5.1.2	5.1.2SR1

Unified IP Phone 6901

Cisco Session Initiation Protocol(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）
SIP v.9	9.3(1)SR3

Unified SIP Phone 3905

Cisco Session Initiation Protocol(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）
SIP v.9	9.4(1)SR4

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Techcombank Vietnam社のCuong Van Bui氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uipphone-xss-NcmUykqA

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	2023-NOV-15

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。