マルチプラットフォームファームウェアを搭載したCisco 6800、7800、8800、および9800シリーズの電話機でクロスサイトスクリプティング(XSS)の脆弱性が保存されている

Medium

アドバイザリーID : cisco-sa-mpp-xss-8tAV2TvF
初公開日 : 2024-11-06 16:00
バージョン 1.0 : Final
CVSSスコア : 4.8
回避策 : No workarounds available
Cisco バグ ID : CSCwm39676 CSCwm41666 CSCwm41710 CSCwm41721 CSCwm41656 CSCwm41711 CSCwm38104 CSCwm41657 CSCwm41668 CSCwm41712 CSCwm41723 CSCwm41724 CSCwm41649 CSCwm41715 CSCwm41716 CSCwm41650 CSCwm41651 CSCwm41664

CVE-2024-20533
CVE-2024-20534

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 6800、7800、8800シリーズ、およびCisco Video Phone 8875 with Cisco Multiplatform FirmwareのWeb UIにおける複数の脆弱性により、認証されたリモート攻撃者が、ユーザに対して保存された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。

これらの脆弱性は、該当デバイスのWeb UIでユーザ入力が適切に検証されないことに起因しています。攻撃者は、悪意のあるコードをインターフェイスの特定のページに挿入することで、これら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：これら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おり、攻撃者がデバイスで管理者クレデンシャルを持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-mpp-xss-8tAV2TvF

該当製品

脆弱性のある製品

公開時点で、これらの脆弱性は、Ciscoマルチプラットフォームファームウェアの脆弱性が存在するリリースを実行していて、Webアクセスが有効になっている次のシスコ製品に影響を与えました。

- デスクフォン9800シリーズマルチプラットフォームファームウェア
- 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
- Video Phone 8875マルチプラットフォームファームウェア

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、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- ATA 191アナログ電話アダプタ
- ATA 191および192マルチプラットフォームアナログ電話アダプタ
- IP DECT 6800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 6901
- Unified SIP Phone 3905
- Webex会議室の電話
- Webex Share
- ワイヤレス IP Phone 8821

- Wireless Phone 840および860

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。最新情報については、本アドバイザリ上部のバグIDの「詳細」セクションを参照してください。

左の列にはCiscoソフトウェアリリースが、右の列にはそのリリースが本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、またどのリリースにこれらの脆弱性に対する修正が含まれているかを示します。

Desk Phone 9800シリーズ

Cisco 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）
3.1(1)	3.2(1)
3.1(1)SR1	3.2(1)

IP Phone 6800、7800、8800 シリーズ

Cisco 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）
12.0.5SR1	12.0.6

Video Phone 8875

Cisco 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)
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

Cisco IP Conference Phone 8831 マルチプラットフォーム ファームウェア

マルチプラットフォームファームウェア搭載のCisco IP Conference Phone 8831は、ソフトウェアメンテナンスリリースの終了日を過ぎています。このため、シスコは、このアドバイザリで説明している脆弱性に対処するためのソフトウェアのアップデートをリリースしておらず、今後もリリースする予定はありません。この製品のサポート終了通知を参照することをお勧めします。

マルチプラットフォーム フォンおよびアクセサリ向け Cisco IP Conference Phone 8831 の販売終了およびサポート終了のお知らせ

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

これらの脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のIan Thorne氏による社内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-mpp-xss-8tAV2TvF

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、単独の転載や意訳を施した場合、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。