Cisco IP Phone 6800、7800、および8800シリーズマルチプラットフォームファームウェア Web UIのコマンドインジェクションの脆弱性

High

アドバイザリーID : cisco-sa-20180711-phone-webui-inject

CVE-2018-0341

初公開日 : 2018-07-11 16:00

最終更新日 : 2018-07-12 13:57

バージョン 1.1 : Final

CVSSスコア : 8.8

回避策 : No workarounds available

Cisco バグ ID : CSCvi51426

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

マルチプラットフォームファームウェアを搭載したCisco IP Phone 6800、7800、および8800シリーズのWebベースUIの脆弱性により、認証されたリモートの攻撃者がWebサーバの権限を使用してコマンドインジェクションを実行し、コマンドを実行できる可能性があります。

この脆弱性は、入力に対する不十分な検証に起因します。攻撃者は、特定のユーザ入力フィールドに任意のシェルコマンドを含めることによって、この脆弱性を不正利用する可能性があります。

シスコでは、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する予定です。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-20180711-phone-webui-inject

該当製品

脆弱性のある製品

この脆弱性は、リリース11.2(1)より前のマルチプラットフォームファームウェアリリースを実

行している次のシスコ製品に影響を与えます。

- 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

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。

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

シスコでは、このアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供する予定です。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート（Cisco Security Advisories and Alerts）] 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。

サービス契約をご利用でないお客様

シスコから直接購入したが Cisco Service Contract をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを POS から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

この脆弱性は、2018年8月に利用可能になるファームウェアリリース11.2(1)で修正されています。

ファームウェアのアップデートは、Cisco.comのSoftware Centerからダウンロードできます。**[製品(Products)] > [コラボレーションエンドポイント(Collaboration Endpoints)] > [IPフォン(IP Phones)] > [マルチプラットフォームファームウェア搭載IPフォン(IP Phones with Multiplatform Firmware)]**の順に移動してください。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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を確認していません。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180711-phone-webui-inject

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	修正済みリリースの入手可能性に関する情報を追加。	修正済みソフトウェア	Final	2018年7月12日
1.0	初回公開リリース	-	Final	2018年7月11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。