Cisco IP Phone 8800 シリーズの認証バイパスの脆弱性

High

アドバイザリーID : cisco-sa-20190320-ipab

初公開日 : 2019-03-20 16:00

最終更新日 : 2019-03-22 19:30

バージョン 1.1 : Final

CVSSスコア : 7.5

回避策 : No workarounds available

Cisco バグ ID : CSCvn56175 CSCvo58414

CVE-2019-1763

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 8800 シリーズ Session Initiation Protocol（SIP）ソフトウェアの Web ベース管理インターフェイスの脆弱性により、不正なリモートの攻撃者が認証をバイパスし、重要なサービスにアクセスし、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、ソフトウェアがリクエストを処理する前に URL のサニタイズに失敗することに起因しています。 攻撃者がこの脆弱性を不正利用して、巧妙に細工された URL を送信する可能性があります。 不正利用に成功すると、攻撃者は重要なサービスに不正にアクセスし、DoS 状態を引き起こす恐れがあります。

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ました。 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190320-ipab

該当製品

脆弱性のある製品

以下のリリース以前の SIP ソフトウェアを実行する Cisco IP Phone 8800 シリーズで、Web

サービス機能を有効にしている場合に、この脆弱性の影響を受けます。

- Wireless IP Phone 8821 および 8821-EX 向け 11.0(5)
- IP Conference Phone 8832 および残りの IP Phone 8800 シリーズ向け 12.5(1)SR1

注: Web サービス機能は、SIP ソフトウェアでデフォルトで無効になっています。

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が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

シスコは、この脆弱性が以下のシスコ製品に影響を与えないことを確認しました。

- IP Conference Phone 8831
- マルチプラットフォーム ファームウェアを実行する IP フォン

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しています。 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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、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は新規リリースでも継続して適切なサポートが受けられることを確

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シスコのサービス契約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購入先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、以下の SIP ソフトウェアのリリースでは修正されています。

- Cisco Wireless IP Phone 8821 および 8821-EX 向け 11.0(5)（今後のリリース）
- 残りの Cisco IP Phone 8800 シリーズ向け 12.5(1)SR1 以降

SIP ソフトウェアは、Cisco.com の Software Center にアクセスして次の手順でダウンロードできます。

1. [すべて参照（Browse all）] をクリックします。
2. [コラボレーションエンドポイント（Collaboration Endpoints）] > [IPフォン（IP Phones）] > [IP Phone 8800シリーズ（IP Phone 8800 Series）] > [モデル（Model）] > [Session Initiation Protocol (SIP)ソフトウェア（Session Initiation Protocol (SIP) Software）] を選択します。
3. [Session Initiation Protocol (SIP)ソフトウェア（Session Initiation Protocol (SIP) Software）] ページの左側のペインを使用して、リリースにアクセスします。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

この脆弱性を報告していただいた modzero AG 社の David Gullasch 氏に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190320-ipab

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.1	「脆弱性のある製品」の箇条書きの前書きに Web サービス機能を追加。「脆弱性のある製品」に Web サービスについてのメモを追加。「脆弱性のある製品」から脆弱でない製品に関する重複するメモを削除。「修正済みリリース」に 11.0(5) が今後のリリースであることを示すメモを追加。	「脆弱性のある製品」および「修正済みリリース」	最終版	2019年3月22日
1.0	初回公開リリース		最終版	2019年3月20日

利用規約