Cisco IP 電話の Web アプリケーション バッファ オーバーフローの脆弱性

アドバイザリーID : cisco-sa-20160609-ipp CVE-2016-1421
初公開日 : 2016-06-09 16:00
最終更新日 : 2020-04-16 15:59
バージョン 2.1 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID : CSCuz03034 CSCvs78281

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 電話の Web アプリケーションの脆弱性により、認証されていないリモートの攻撃者がルート権限でコードを実行したり、該当 IP 電話のリロードを引き起こしたりできるようになります。その結果、サービス妨害（DoS）状態に陥る可能性があります。

この脆弱性は、該当ソフトウェアが入力データの範囲をチェックできないことに起因します。攻撃者は、ターゲットデバイスの Web サーバに巧妙に細工された HTTP リクエストを送信することにより、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者がルート権限でリモートからコードを実行したり、該当 IP 電話のリロードを引き起こしたりできるようになり、その結果として DoS 状態に陥る可能性があります。

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-20160609-ipp

該当製品

脆弱性のある製品

この脆弱性は、Web アクセスが有効になっており、そのデバイス向けの最初の修正リリースより前の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 7811、7821、7841、7861 デスクトップフォン
- IP Phone 8811、8841、8845、8851、8861、8865 デスクトップフォン
- Wireless IP Phone 8821 および 8821-EX

注：Webアクセスはデフォルトで無効になっています。管理者は、[デバイス（Device）] > [電話の選択（Select a Phone）] の順に選択して [Webアクセス（Web Access）] が [有効（Enabled）] と [無効（Disabled）] のどちらに設定されているのかをチェックすることにより、Cisco Unified Communications Manager から Web アクセスの設定を確認できます。[無効（Disabled）] に設定されている場合、IP 電話に脆弱性はありません。

脆弱性のある Cisco ファーム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。

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 アナログ電話アダプタ
- ATA 191 Analog Telephone Adapter
- ATA 192 マルチプラットフォーム アナログ電話アダプタ
- 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 DECT 6825 マルチプラットフォーム ファームウェア
- IP Phone 6821、6841、6851、6861、6871 マルチプラットフォーム ファームウェア
- IP Phone 7811、7821、7841、7861 デスクトップフォン（マルチプラットフォーム ファームウェア搭載）
- IP Phone 8811、8841、8845、8851、8861、8865 デスクトップフォン（マルチプラットフォーム ファームウェア搭載）
- SPA112 2 ポート電話アダプタ
- SPA122 ルータ内蔵 ATA
- SPA2102 ルータ内蔵電話アダプタ
- SPA232D Multi-Line DECT ATA
- SPA3102 ルータ内蔵音声ゲートウェイ
- SPA8000 8ポートIPテレフォニーゲートウェイ
- SPA8800 IP テレフォニーゲートウェイ（4 FXS ポートと 4 FXO ポートを内蔵）
- Small Business SPA300 シリーズ IP フォン
- Small Business SPA500 シリーズ IP フォン
- Unified IP Conference Phone 8831

- サードパーティコール制御向け Unified IP Conference Phone 8831
- Unified IP 電話 6901 および 6911
- Unified SIP Phone 3905

回避策

この脆弱性に対処する回避策はありません。

ただし、Web アクセスが必要ない場合、設定の無効化はこの脆弱性の緩和策とみなされます。Web アクセスが無効になっている場合、その電話に脆弱性はありません。詳細については、『Phone Hardening 』の「Web Access Disable」の章を参照してください。

注：Cisco IP Phoneでは、Webアクセスはデフォルトで無効になっています。

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リリースしています。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、アクセスまたはその他の方法で使用した場合、お客様は https://www.cisco.com/c/en/us/products/end-user-license-agreement.html に記載の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。

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

次の表に示すように、該当する修正済みの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。

Cisco IP Phone モデル	Cisco Bug ID	First Fixed Release（修正された最初のリリース）
IP Phone 7811、7821、7841、7861 デスクトップフォン	CSCuz03034	11.7(1)
IP Phone 8811、8841、8845、8851、8861、8865 デスクトップフォン	CSCuz03034	11.7(1)
Wireless IP Phone 8821、8821-EX	CSCvs78281	11.0(5)SR3

Cisco.comのSoftware CenterからCisco IP Phoneのファームウェアをダウンロードするには、次の手順を実行します。

1. [すべてを参照（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）] を選択します。
3. 製品セレクタの右ペインから特定の製品を選択します。
4. 製品ページの左ペインからリリースを選択します。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、アドバイザリで説明されている脆弱性に対して概念実証段階のエクスプロイト コードが入手可能であることを認識しています。

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。また、この脆弱性を報告していただいた Tenable 社の Jacob Baines 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160609-ipp

改訂履歴

バージョン	説明	セクション	ステータス	日付
2.1	初回公開リリース	公開悪用コードが存在することを示すために「不正利用と公表」を更新。	Final	2020 年 4 月 16 日
2.0	CVSSv3 スコアの情報、SIR、影響、脆弱性のある製品、および修正済みリリースを更新。緩和策と功績が認められた外部の研究者を追加。	タイトル、ヘッダー、概要、脆弱性のある製品、脆弱性のない製品、回避策、修正済みソフトウェア、ソース	Final	2020 年 4 月 15 日
1.0	初回公開リリース	—	Final	2016 年 6 月 9 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。