Cisco Small Business SPA50x、SPA51x、SPA52x シリーズ IP フォン SIP におけるサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20171018-sip1

初公開日 : 2017-10-18 16:00

バージョン 1.0 : Final

CVSSスコア : 7.5

回避策 : No workarounds available

Cisco バグ ID : CSCvc63986

CVE-2017-12260

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 Small Business SPA50x、SPA51x、SPA52x シリーズ IP フォンの Session Initiation Protocol（SIP）機能の実装における脆弱性により、認証されていないリモート攻撃者により、該当デバイスが応答しなくなる状況が引き起こされ、その結果、サービス妨害（DoS）状態になる可能性があります。

本脆弱性は、該当デバイスでの SIP 要求メッセージの不適切な処理に起因するものです。 攻撃者が、該当デバイスに SIP ペイロードを送信する際に、フォーマット指定子を使用することで、本脆弱性が不正利用されます。 不正利用に成功すると、攻撃者によって該当デバイスが応答しなくなる状況が引き起こされ、その結果、デバイスを手動で再起動するまで DoS 状態が続くことになります。

シスコでは、本脆弱性に対処するファームウェア 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。
018-sip1

該当製品

脆弱性のある製品

本脆弱性は、ファームウェア リリース 7.6.2SR1 以前を実行する Cisco Small Business

SPA50x、SPA51x、SPA52x シリーズ IP フォンに影響を及ぼします。

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

詳細

セキュリティ侵害の痕跡

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。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.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。

http://www.cisco.com/en/US/support/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

Cisco Small Business SPA50x シリーズ IP フォンおよび Cisco Small Business SPA51x シリーズ IP フォンに対しては、ファームウェア リリース 7.6.2SR2 以降で、本脆弱性を修正しています。顧客はファームウェアリリースに Cisco.com の Software Center にアクセスすることおよび**コラボレーション エンドポイント > IP フォン > Small Business SPA500 シリーズ IP Phone > *IP電話モデル* > IP Telephone ファームウェア**へのナビゲートによってアップグレードする必要があります。

Cisco Small Business SPA52x シリーズ IP フォンに対しては、本脆弱性を修正するファームウェアはまだ用意されていません。 該当するファームウェアに対するアップデートは、用意でき次第リリースします。 また、アップデートが公開された際には、本アドバイザリの情報も更新されます。

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

この脆弱性は内部テストで発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171018-sip1

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017 年 10 月 18 日

利用規約

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。