Cisco Small Business SPA300およびSPA500シリーズのIP Phoneにおける認証されていないリモートダイヤルの脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20150319-CVE-2015-0670 **初公開日 :** 2015-03-19 21:04 **最終更新日 :** 2015-03-25 18:43 **バージョン 2.0 :** Final **CVSSスコア :** 6.4 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCuo52482	CVE-2015-0670

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 SPA 300および500シリーズIPフォンのファームウェアの脆弱性により、認証されていないリモートの攻撃者がIPフォンのオーディオストリームをリッスンできる可能性があります。

この脆弱性は、デフォルト設定の認証設定が不適切であることに起因します。攻撃者は、巧妙に細工されたXML要求を該当デバイスに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。この不正利用により、攻撃者はリモートで音声ストリームを聞いたり、電話をかけたりできる可能性があります。

シスコは脆弱性を確認しましたが、ソフトウェアアップデートは利用できません。

この脆弱性をエクスプロイトするには、攻撃者がファイアウォールの背後にある信頼できる内部ネットワークにアクセスし、巧妙に細工されたXML要求をターゲットデバイスに送信する必要があります。このアクセス要件により、不正利用が成功する可能性が低くなる可能性があります。

シスコは、この脆弱性を報告していただいたTech AnalysisのChris Watts氏に感謝いたします。

シスコは、この脆弱性に対処する新しいソフトウェアを2015年4月10日までにリリースする予定です。

該当製品

シスコは、登録ユーザ向けにバグID CSCuo52482をリリースしました。このバグには、影響を受ける製品バージョンの詳細と最新リストが含まれています。

脆弱性のある製品

このアラートが最初に公開された時点では、Cisco Small Business SPA300およびSPA500シリーズIP Phoneバージョン7.5.5には脆弱性が存在していました。Cisco Small Business SPA300およびSPA500シリーズIP Phoneの新しいバージョンにも脆弱性が存在する可能性があります。

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。

回避策

今後のアップデートやリリースについては、ベンダーに連絡することを推奨します。

管理者は、該当するデバイスの設定でXML実行認証を有効にすることを推奨します。

信頼できるユーザだけにネットワークアクセスを許可することを推奨します。

管理者は、堅実なファイアウォール戦略を使用して、影響を受けるシステムを外部からの攻撃から保護できます。

IPベースのアクセスコントロールリスト(ACL)を使用して、信頼できるシステムだけに該当システムへのアクセスを許可することを検討することもできます。

影響を受けるシステムを監視することを推奨します。

修正済みソフトウェア

ソフトウェアの更新プログラムは利用できません。

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。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-

20150319-CVE-2015-0670

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	Cisco Small Business SPA 300および500シリーズIPフォンには、認証されていないリモートの攻撃者が機密情報にアクセスできる可能性のある脆弱性が存在します。更新プログラムは利用できません。	適用外	Final	2015年3月19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。