

Cisco Unified Customer Voice Portal の自動音声応答接続におけるサービス妨害の脆弱性



アドバイザリーID : cisco-sa-20180221-cvp [CVE-2018-](#)

初公開日 : 2018-02-21 16:00

[0139](#)

バージョン 1.0 : Final

CVSSスコア : [8.6](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCve70560](#)

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 Unified Customer Voice Portal (CVP) の自動音声応答 (IVR) 管理接続インターフェイスの脆弱性により、未認証のリモート攻撃者によって IVR 接続が切断され、システム全体がサービス妨害 (DoS) 状態に陥る可能性があります。

この脆弱性は、IVR 接続がすでに確立されているときに TCP 接続要求が不適切に処理されることに起因します。この脆弱性は、標的とされた CVP デバイスの IP アドレスに宛てて、細工を施した接続を開始されることにより、不正利用される可能性があります。不正利用されると、IVR から CVP への接続が切断され、CVP が新たな着信コールを受けられなくなる一方で IVR は自動的に CVP との接続の再確立を試みる、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。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180221-cvp>

該当製品

脆弱性のある製品

この脆弱性は、Cisco Unified Customer Voice Portal (CVP) ソフトウェア リリース 11.5(1) に影響します。

実行されている Cisco Unified CVP ソフトウェア リリースの判別は、管理者が Web ブラウザ

を使用して HTTPS 経由で Cisco Unified CVP クライアントに接続することによって実施できません。リリース番号はソフトウェアのホームページに表示されています。ホームページに表示されるテキストの例を下記に示します。

<#root>

Cisco Unified Customer Voice Portal

Version 11.5(1)

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。

セキュリティ侵害の痕跡

システム ログ ファイル内に次のメッセージがある場合、この脆弱性が不正利用されている可能性が考えられます。

```
%CVP_11_5_ICM-3-LOGMSG_ICM_SS_GENERAL_INFO: 新しいVRU PIM接続SYN  
RemoteAddress=x.x.x.x,RemotePort=aaaa, LocalAddress=y.y.y.y,LocalPort=bbbb
```

```
%CVP_11_5_ICM-3-LOGMSG_ICM_SS_PIM_SHUTDOWN: VRU PIM接続が削除されました  
: RemoteAddress=x.x.x.x,RemotePort=aaaa, LocalAddress=y.y.y.y,LocalPort=bbbb
```

システム ログ ファイル内にこれらのメッセージが存在している場合は、Cisco Technical Assistance Center (TAC) に連絡し、システム ログ ファイルを精査して、デバイスがこの脆弱性の不正利用による侵害を受けているかどうか確認してください。

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です。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 (https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html) に連絡してアップグレードを入手してください。

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、Cisco Unified Customer Voice Portal ソフトウェア リリース 11.6(1) 以降で修正されています。このソフトウェアは、Cisco.com の [Software Center からダウンロードできます](#)。ダウンロードするには、[製品 (Products)] > [カスタマーコラボレーション (Customer Collaboration)] > [コンタクトセンターソリューションのオプション (Options for Contact Center Solutions)] > [Unified Customer Voice Portal] > [Cisco Customer Voice Portalソフトウェアリリース11.6(1) (Cisco Customer Voice Portal Software Releases-11.6(1))] の順にアクセスします。

この脆弱性の修正プログラムは、Cisco Unified Customer Voice Portal ソフトウェア リリース 11.5(1) Engineering Special (ES) 12 にも含まれています。このソフトウェアは、Cisco.comの Software Center([Cisco Unified Customer Voice Portal Software Release 11.5\(1\) ES12](#))から入手できます。

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

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180221-cvp>

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	初回公開リリース	—	Final	2018 年 2 月 21 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、単独の転載や意識を施した場合、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。