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

High

アドバイザリーID : cisco-sa-20180221-cvp

初公開日 : 2018-02-21 16:00

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

CVE-2018-0139

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。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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://tools.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す。 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。

```
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: new VRU PIM connection 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 connection removed: 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。
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、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 から入手できます。 Cisco Unified Customer Voice Portal ソフトウェア リリース 11.5(1)_ES12

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、Cisco TAC のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180221-cvp

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018 年 2 月 21 日

利用規約