Cisco Unified Customer Voice Portal における Denial of Service（DoS）の脆弱性

High

アドバイザリーID： cisco-sa-20180117-cvp
初公開日： 2018-01-17 16:00
最終更新日： 2018-02-15 20:49
バージョン 1.1： Final
CVSSスコア： 8.6
回避策： No workarounds available
Cisco バグ ID： CSCve85840

CVE-2018-0086

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）のアプリケーション サーバの脆弱性により、認証されていないリモート攻撃者が該当デバイスにサービス妨害（DoS）状態を引き起こす可能性があります。

この脆弱性は、Cisco Virtualized Voice Browser（VVB）との通信中に CVP が受信した不正な SIP INVITE トラフィックに起因するものです。 この脆弱性は、攻撃者がターゲット アプライアンスに不正な形式の SIP INVITE トラフィックを送信することによって、不正利用される可能性があります。 不正利用されると、攻撃者がデバイス上のサービスとデータの可用性に影響を与え、DoS 状態を引き起こすことが可能になります。

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-20180117-cvp

該当製品

脆弱性のある製品

この脆弱性は、11.6(1) より前のソフトウェア リリースを実行している Cisco Unified CVP 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。

回避策

この脆弱性に対処する回避策はありませんが、 脆弱性を軽減する方法はあります。

1) Cisco UCCE（Unified Contact Center Enterprise）インフラストラクチャに対し、受信する SIP トラフィックを、信頼できる IP アドレスからのものだけに限定する設定を行います。

2) CVP と ISP 間に存在するサードパーティ製ゲートウェイで、不正な SIP ヘッダーや悪意のある情報が含まれたパケットをドロップするコンテンツ フィルタリングを有効にします。

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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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

次の表の最初の列に Cisco Unified CVP ソフトウェアのメジャー リリースを、2 番目の列にこの脆弱性に対処するためにインストールする推奨リリースを示します。

次の表に示すように、適切なリリースにアップグレードする必要があります。

Cisco Unified CVP メジャーリリース	Ciscoバグ CSCve85840 のための修正済みリリース
10.5	影響あり。 11.6 へ移行してください
11.0	影響あり。 11.6 へ移行してください
11.5	影響あり。 11.6 へ移行してください
11.6	Not affected

アクティブなサービス サービス契約を持つ顧客はナビゲートによって Cisco.com の Software Center からの **ダウンロード ホーム > 製品 > カスタマ コラボレーション > コンタクト センター ソリューションのオプション > Unified Customer Voice Portal** にメジャーリリースのための修正済みソフトウェアをダウンロードできます。

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、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-20180117-cvp

改訂履歴

Version	Description	Section	Status	日付
1.1	修正済みソフトウェアの表を追加。	修正済みソフトウェア	Final	2018 年 2 月 15 日
1.0	初回公開リリース		Final	2018 年 1 月 17 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。