Cisco Unified Customer Voice Portal オペレーション コンソール 特権 拡大脆弱性

High

アドバイザリーID : cisco-sa-20170920-cvp

初公開日 : 2017-09-20 16:00

最終更新日 : 2017-09-22 15:36

バージョン 1.2 : Final

CVSSスコア : 8.8

回避策 : No workarounds available

Cisco バグ ID : CSCve92752

CVE-2017-12214

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

オペレーション、管理、メンテナンスおよびプロビジョニング（OAMP）Cisco Unified Customer Voice Portal（CVP）のためのクレデンシャル リセットの脆弱性は機能高度な特権を得る認証される、リモート攻撃者可能にする可能性があります。

脆弱性は適切な入力の検証の欠如が原因です。 攻撃者は OAMP にによって認証および巧妙に細工された HTTP 要求を送信 することこの脆弱性を不正利用する可能性があります。 正常な工クスプロイトは攻撃者が *アドミニストレーター特権*を得ることを可能にする可能性があります。 攻撃者はシステムにこの脆弱性を不正利用するために認証に成功する必要があります。

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-20170920-cvp

該当製品

脆弱性のある製品

この脆弱性はソフトウェア リリース 10.5、11.0、または 11.5 を実行する Cisco Unified Customer Voice Portal（CVP）に影響を与えます。

Cisco Unified CVP ソフトウェアのどのリリースが動作しているか判別するために、管理者は HTTPS によって Cisco Unified CVP クライアントに接続するのに Webブラウザを使用できます。 リリース番号はソフトウェア ホームページで現われます。 以下はホームページで出るかもしれないテキストの例です:

```
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。

侵害のインジケーター

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

この脆弱性は Cisco Unified Customer Voice Portal ソフトウェア リリース 11.6 または それ 以降で解決されます。 ソフトウェアは Cisco.com の Software Center から **ダウンロード ホーム > 製品 > カスタマー 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** へのによってナビゲート ダウンロードすることができます。

注: リリース トレイン 10.5、11.0、および 11.5 のために利用可能 な エンジニアリング スペシャル（ES）があります。 これらの ES リリースに関しては Cisco TAC に、Cisco.com の Software Center から利用可能ではない、連絡して下さいまたは次の場所からリリースをダウンロードして下さい。
Cisco Unified CVP 10.5(1)_ES31 に関しては- リリース 10.5(1)_ES31
注: CVP 10.5(1)_ES31 をインストールするために、前パッチ CVP 10.5(1)_ES23 は必須で、最初に展開する必要があります。

Cisco Unified CVP 11.0(1)_ES27 に関しては- リリース 11.0(1)_ES27
注: CVP 11.0(1)_ES27 をインストールするために、前パッチ CVP 11.0(1)_ES8 は必須で、最初に展開する必要があります。

Cisco Unified CVP 11.5_ES13 に関しては- リリース 11.5(1)_ES13

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サポート例の解決の間に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170920-cvp

改訂履歴

Versio	Description	Section	Statu	日付

n			s	
1.2	エンジニアリング スペシャルに関する詳細追加される修正済みソフトウェアの下およびアップグレードする方法を。	修正済みソフトウェア。	Final	2017-September-22
1.1	特派員を設計する 11.5(1)_ES13 へのハイパー リンクは訂正されました。	修正済みソフトウェア	Final	2017-September-21
1.0	Initial public release.		Final	2017-September-20

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。