シスコ クラウド サービス プラットフォーム 2100 における不正アクセスの脆弱性

Critical

アドバイザリーID : cisco-sa-20171018-ccs

初公開日 : 2017-10-18 16:00

バージョン 1.0 : Final

CVSSスコア : 9.9

回避策 : No workarounds available

Cisco バグ ID : CSCve64690

CVE-2017-12251

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

シスコ クラウド サービス プラットフォーム（CSP）2100 の Web コンソールの脆弱性によって、認証済みのリモート攻撃者が、該当の CSP デバイス上でリモートから動作するサービスもしくは仮想マシン（VM）と不正にやりとりできる可能性があります。

本脆弱性は、Web コンソールの URL における特定の認証メカニズムの生成に脆弱性があることに起因します。 攻撃者が、Cisco CSP でホストされる VM の URL をブラウザで参照し、Web アプリケーションの認証制御のメカニズムを定める特定のパターンを確認することで、本脆弱性を不正に利用できる可能性があります。 不正利用により、攻撃者が CSP 上の特定の VM にアクセスできる可能性があり、その結果、システムの機密性、整合性、可用性が完全に失われます。

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-20171018-ccs

該当製品

脆弱性のある製品

本脆弱性は、ソフトウェア リリース 2.1.0、2.1.1、2.1.2、2.2.0、2.2.1、2.2.2 のいずれかを実行しているシスコ クラウド サービス プラットフォーム（CSP）2100 に影響を及ぼします。

Cisco CSP 2100 のどのソフトウェア リリースを実行しているか判別するために、管理者は CLI のユーザ EXEC コマンド モードの **show version コマンドを**発行できます。 以下は、CLI で返されるテキストの例です。

```
csp# show version
Cisco クラウド サービス プラットフォーム ソフトウェア、2100 ソフトウェア ( CSP-2100 )、 バージョン 2.0.0 Build:6
TAC support: http://www.cisco.com/tac
Copyright (c) 2015 by Cisco Systems, Inc.
Compiled Wednesday 10-February-2016 14:48
csp#
```

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。

詳細

セキュリティ侵害の痕跡

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

本脆弱性は、シスコ クラウド サービス プラットフォームのリリース 2.2.3 以降で修正されています。 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 > スイッチ > 仮想ネットワーキング > Cloud Services Platform 2100** 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。

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

本脆弱性は、MWR InfoSecurity のシニア セキュリティ コンサルタント Chris Day 氏によって報告されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171018-ccs

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017 年 10 月 18 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。