Cisco Common Services Platform Collector のスタティック クレデンシャルの脆弱性

アドバイザリーID : cisco-sa-20190313-cspcscv
初公開日 : 2019-03-13 16:00
バージョン 1.0 : Final
CVSSスコア : 9.8
回避策 : Yes
Cisco バグ ID : CSCvo38510

CVE-2019-1723

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 Common Services Platform Collector（CSPC）の脆弱性により、認証されていないリモート攻撃者がデフォルトの静的パスワードが設定されたアカウントを使用して該当デバイスにアクセスできるようになります。このアカウントには 管理者権限はありません。

この脆弱性は、影響を受けるソフトウェアにデフォルトの静的パスワードが設定されたユーザ アカウントがあるために存在します。攻撃者は、このアカウントを使用して該当システムにリモート接続することにより、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者はデフォルト アカウントを使用して CSPC にログインできるようになります。

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。本脆弱性に対処する回避策がいくつかあります。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190313-cspcscv

該当製品

脆弱性のある製品

この脆弱性は、Cisco CSPC リリース 2.7.2 ~ 2.7.4.5 と 2.8.1.2 より前の 2.8x リリースのすべてに影響を与えます。

管理者は、show version コマンドを使用することにより、デバイスで実行されているリリースを確認できます。Release 2.8.1 を実行している CSPC の出力例は、次のようになります。

```
<#root>

admin#

show version

    Build-name    : Collection Platform Software 2.8.1

    Version       : sp-30.1.1-0-0-lnx64
admin#
```

注：Cisco Smart Net Total Care(SmartNet)Network CollectorおよびCisco Partner Support Service(PSS)Network CollectorはCisco CSPCを使用します。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

回避策

回避策に関して支援が必要な場合、お客様は Cisco Technical Assistance Center（TAC）でサービス リクエストをオープンするか、Cisco Network Optimization Service（NOS）または Cisco Business Critical Services（BCS）に登録しているのであれば、プライマリ ネットワーク コンサルティング エンジニアに問い合わせることが可能です。

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、[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 Cisco Service Contract 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 POS 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

Cisco CSPC 2.7.x に関しては、リリース 2.7.4.6 でこの脆弱性を修正済みです。

Cisco CSPC 2.8.x に関しては、リリース 2.8.1.2 でこの脆弱性を修正済みです。

Cisco CSPC のファームウェアは、Cisco.com の Software Center から次の手順でダウンロードできます。

1. [すべてを参照（Browse All）] をクリックします。
2. [クラウドおよびシステム管理（Cloud and Systems Management）] > [サービス（Services）] > [Common Services Platform Collector（CSPC）（Common Services Platform Collector (CSPC)）] の順に選択します。
3. [Common Services Platform Collector（CSPC）（Common Services Platform Collector (CSPC)）] ページの左ペインからリリースにアクセスします。

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

この脆弱性を報告していただいた David Coomber 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190313-cspcscv

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	2019 年 3 月 13 日

利用規約

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。