Cisco Prime Collaboration Provisioning におけるハードコードされたパスワードによる脆弱性

Critical

アドバイザリーID : cisco-sa-20180307-cpcp

初公開日 : 2018-03-07 16:00

バージョン 1.0 : Final

CVSSスコア : 5.9

回避策 : No workarounds available

Cisco バグ ID : CSCvc82982

CVE-2018-0141

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 Prime Collaboration Provisioning（PCP）ソフトウェアにおける脆弱性により、未認証のローカル攻撃者が、基盤となる Linux オペレーティング システムにログインできてしまう可能性があります。

アカウント パスワードがシステム上にハードコードされていることが原因です。 攻撃者は、ハードコードされたクレデンシャルを使用して、セキュア シェル（SSH）で該当システムに接続することで、この脆弱性を不正利用する可能性があります。 不正利用に成功すると、権限の低いユーザとして、基盤となるオペレーティング システムにアクセスできる可能性があります。 攻撃者は、低レベルの権限を取得した後、 *ルート*権限に昇格してデバイスを完全に制御できるようになる可能性があります。

注： この脆弱性の共通脆弱性評価システム（CVSS）ベース スコアは 5.9 で、通常は中レベルのセキュリティ影響評価（SIR）が割り当てられます。ただし、攻撃者が *root* 権限に昇格できてしまうという状況が考慮され、 SIR は「緊急」に設定されています。

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-20180307-cpcp

該当製品

脆弱性のある製品

この脆弱性の影響を受けるのは、Cisco Prime Collaboration Provisioning（PCP）ソフトウェア リリース 11.6 のみです。 それより前のビルドは、この脆弱性の影響を受けません。

Cisco PCP 11.6 および 12.1 では、管理者が GUI から以下の操作を行うことで現在の PCP ソフトウェア リリースを確認することができます。

1. PCP にログインします。
2. 画面の右上近くにある設定アイコンをクリックします。
3. [バージョン情報（About）] をクリックします。

リリース情報は、ログイン画面にも表示されます。

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。

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 Prime Collaboration Provisioning ソフトウェア リリース 12.1 移行で修正されています。
このソフトウェアは Cisco.com の Software Center でダウンロードできます（[製品（Products）] > [クラウドおよびシステム管理（Cloud and Systems Management）] > [コラボレーションとユニファイド コミュニケーションの管理（Collaboration and Unified Communications Management）] > [Prime Collaboration]）。

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、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-cpcp

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018 年 3 月 7 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。