Cisco Prime License Manager の特権昇格の脆弱性

アドバイザリーID : cisco-sa-cisco-prime-priv-esc-HyhwdzBA
初公開日 : 2020-07-15 16:00
バージョン 1.0 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID : CSCvq97227

CVE-2020-3140

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 License Manager（PLM）ソフトウェアの Web 管理インターフェイスの脆弱性により、認証されていないリモートの攻撃者が該当デバイスに不正にアクセスする可能性があります。

この脆弱性は、Web 管理インターフェイスでユーザが行った入力の検証が不十分であることに起因します。攻撃者は、該当システムに悪意のあるリクエストを送信することにより、この脆弱性をエクスプロイトする可能性があります。このエクスプロイトにより、攻撃者はシステムの管理者レベルの権限を取得する可能性があります。攻撃者がこの脆弱性をエクスプロイトするには、有効なユーザ名が必要です。

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。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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-prime-priv-esc-HyhwdzBA

該当製品

脆弱性のある製品

この脆弱性は、次の Cisco PLM ソフトウェアリリースに影響を与えます。

- 10.5(2)SU9 以前
- 11.5(1)SU6 以前

Cisco PLM ソフトウェアのスタンドアロン環境と共存環境の両方が影響を受けます。共存環境では、Cisco PLM ソフトウェアは、Cisco Unified Communications Manager（Unified CM）ソフトウェア、Cisco Unified CM Session Management Edition（SME）ソフトウェア、および Cisco Unity Connection ソフトウェアの一部としてインストールされます。

管理者は、Cisco PLM の GUI にログインして右上隅にある [情報（About）] をクリックすることにより、実行している Cisco PLM のリリースを確認できます。

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。

共存インストールの場合、この脆弱性を利用して取得できるのは Cisco PLM へのアクセスのみです。この脆弱性により、Cisco Unified CM ソフトウェア、Cisco Unified CM SME ソフトウェア、または Cisco Unity Connection ソフトウェアへのアクセスが提供されることはありません。

Cisco Unified CM ソフトウェア、Cisco Unified CM SME ソフトウェア、および Cisco Unity Connection ソフトウェアリリース 12 以降は、この脆弱性の影響を受けないことが確認されています。リリース 12 では、ライセンスモデルがスマートライセンスモデルに変更され、Cisco PLM はこれらのリリースに含まれなくなりました。これらの製品を脆弱性が存在するリリースからアップグレードする場合、Cisco PLM をアンインストールする必要はありません。

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 https://www.cisco.com/c/en/us/products/end-user-license-agreement.html に記載の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。

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 セキュリティ アドバイザリ 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アップグレード ソリューション一式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（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

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、次の Cisco PLM ソフトウェア、Cisco Unified CM ソフトウェア、Cisco Unified CM SME ソフトウェア、および Cisco Unity Connection ソフトウェアリリースで修正されています。

- 10.5(2)SU10 以降
- 11.5(1)SU7 以降

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 AdventHealth の Adam Engle 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-prime-priv-esc-HyhwdzBA

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	2020 年 7 月 15 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。

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。