Cisco Prime License Manager SQL インジェクション脆弱性

Critical

アドバイザリーID : cisco-sa-20181128-plm-sql-inject

CVE-2018-15441

初公開日 : 2018-11-28 16:00

最終更新日 : 2018-12-20 15:33

バージョン 1.3 : Final

CVSSスコア : 9.4

回避策 : No workarounds available

Cisco バグ ID : CSCvk30822

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

更新（2018 年 12 月 20 日）：v1.0 パッチで特定された機能上の問題を回避できる、最新のパッチ **ciscocm.CSCvk30822_v2.0.k3.cop.sgn** が Cisco.com で公開されています。 詳細については、「修正済みリリース」セクションを参照してください。

更新（2018 年 12 月 10 日）：**ciscocm.CSCvk30822_v1.0.k3.cop.sgn** パッチをインストールすると、機能上の問題が生じる可能性があります。 これらの問題の一部に対して有効な回避策があります。 「修正済みリリース」セクションで説明しているようにこのパッチをロール バックすると、これらの機能上の問題は修正されますが、デバイスにこのパッチが適用されていない場合は、再びこの脆弱性の影響を受けることになります。 詳細については、「修正済みリリース」セクションを参照してください。

Cisco Prime License Manager（PLM）の Web フレームワーク コード内脆弱性により、認証されていないリモートの攻撃者が任意の SQL クエリを実行できる可能性があります。

この脆弱性は、SQL クエリ内のユーザ入力を正しく検証できないことに起因します。 この脆弱性は、悪意のある SQL ステートメントが含まれている、巧妙に細工された HTTP POST リクエストを攻撃者が該当アプリケーションに送信することによって不正利用される可能性があります。 不正利用に成功すると、攻撃者は PLM データベース内の任意のデータの変更や削除が可能になります。または、 *postgres* ユーザの権限を利用してシェルにアクセス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ました。 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-20181128-plm-sql-inject

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 License Manager リリース 11.0.1 以降です。 Cisco Prime License Manager のスタンドアロン展開、および Cisco Unified Communications Manager や Cisco Unity Connection のインストールの一環として自動的に Cisco Prime License Manager がインストールされる共存展開の両方が影響を受けます。

管理者は、Cisco Prime License Manager GUI にログインし画面の右上隅にある [情報（About）] をクリックして、実行している Cisco Prime License Manager のリリースを特定できます。 次の例は、11.5.1 を実行している Cisco Prime License Manager インスタンスにより報告された**バージョン文字列**を示しています。

バージョン： 11.5.1.10000-5

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が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

Cisco Unified Communications Manager と Cisco Unity Connection のリリース 12.0 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。これは、Cisco Prime License Manager がこれらのリリースに含まれなくなったためです。

回避策

この脆弱性に対処する回避策はありません。

Cisco Unified Communications Manager または Cisco Unity Connection の一部として Cisco Prime License Manager の共存展開を行い、PLM を使用しないお客様は、攻撃ベクトルを封じる機能を次のように無効化できます。

1. Cisco Unified Communications Manager または Cisco Unity Connection CLI に *管理ユーザ*としてログインします。
2. コマンド **license management system remove** を実行します。
3. **y で確認します。**

4. 操作が完了するのを待ちます。 その後、**システムが自動的に再起動します。**

注: この手順は、クラスタ内のすべてのノードで実行する必要があります。 これは、アップグレード実行後も保持されます。

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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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 License Manager パッチ **ciscocm.CSCvk30822_v2.0.k3.cop.sgn** で修正されました（このパッチの v1.0 リリースは、このパッチ自身が原因となって起こる機能上の問題のため利用できなくなっています）。 同じ COP ファイルを、Cisco Unified Communications Manager のスタンドアロン展開、Cisco Unified Communications Manager および Cisco Unity Connection の一部としての共存展開、および影響を受けるすべてのバージョンで使用できます。 インストール手順は、対応する **Readme** ドキュメントに記載されています。

注: このパッチは、Cisco Prime License Manager、Cisco Unified Communications Manager および Cisco Unity Connection 11.5(1) のみにインストールできます。 以前のリリースを実行しているお客様は、このパッチをインストールする前に 11.5(1) にアップグレードする必要があります。

v1.0 パッチ ファイルで特定された機能上の問題

スタンドアロンまたは共存の PLM に **ciscocm.CSCvk30822_v1.0.k3.cop.sgn** パッチをインストールすると、このアドバイザリで説明している脆弱性が解決されますが、この操作により以下の機能が無効になります。

- PLM GUI におけるインストール/アップグレード機能
- PLM GUI におけるバックアップおよび復元機能

機能上の問題の回避策

スタンドアロン PLM

- インストール/アップグレードは、CLI を使用して実行できます。
- バックアップおよび復元機能の回避策はありません。

共存 PLM

- インストール/アップグレードは、CUCM/CUC GUI を使用して実行できます。
- バックアップおよび復元機能は、CUCM/CUC GUI で引き続き使用可能です。

v1.0 パッチから v2.0 パッチへのアップグレード

パッチ **ciscocm.CSCvk30822_v1.0.k3.cop.sgn** を以前インストールしたお客様は、パッチ **ciscocm.CSCvk30822_v2.0.k3.cop.sgn** にアップグレードして機能上の問題を修正する必要があります。 v2.0 パッチをインストールすると、最初に v1.0 パッチがロールバックされた後、v2.0 パッチがインストールされます。

- このアドバイザリの「パッチおよびパッチ ロールバック ファイルのダウンロード」セクションで示されている場所から **ciscocm.CSCvk30822_v2.0.k3.cop.sgn** ファイルをダウンロードします。
- ダウンロードしたファイルを、CLI（スタンドアロン PLM）または CUCM/CUC GUI（共存 PLM）を使用してインストールします。

パッチおよびパッチ ロールバック ファイルのダウンロード

パッチ ファイルおよびパッチ ロールバック ファイル（ **Readme** ドキュメントを含む）は、

Cisco.com の Software Center で、次の場所に移動してダウンロードできます。

Cisco Prime License Manager
[すべてのサポート製品（Browse all）] > [クラウドおよびシステム管理（Cloud and Systems Management）] > [コラボレーションおよびユニファイドコミュニケーション管理（Collaboration and Unified Communications Management）] > [Prime License Manager] > [Prime License Manager 11.5] > [Prime License Manager Software Patches] > [UTILS]

Cisco Unified Communications Manager
[すべてのサポート製品（Browse all）] > [ユニファイドコミュニケーション（Unified Communications）] > [コール制御（Call Control）] > [Unified Communications Manager (CallManager)] > [Unified Communications Managerバージョン11.5（Unified Communications Manager Version 11.5] > [Unified Communications Manager]/[CallManager]/[Cisco Unity Connection Utilities] > [COP-Files]

Cisco Unity Connection
[すべてのサポート製品（Browse all）] > [ユニファイドコミュニケーション（Unified Communications）] > [ユニファイドコミュニケーションアプリケーション（Unified Communications Applications）] > [メッセージング（Messaging）] > [Unity Connection] > [Unity Connectionバージョン11.x（Unity Connection Version 11.x）] > [Unified Communications Manager]/[CallManager]/[Cisco Unity Connection Utilities] > [COP-Files]

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

シスコは、この脆弱性の検出と報告にあたり、Saudi Information Technology Company のセキュリティ調査担当者 Suhail Alaskar 氏に謝意を表します。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181128-plm-sql-inject

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.3	更新された COP ファイルに関する情報を追加。	要約、修正済み固定リリース	最終版	2018年

				12月20日
1.2	初期状態の COP ファイルで発見された機能上の問題に関する追加情報	要約、修正済み固定リリース	Interim	2018年12月10日
1.1	PLM の共存インストールを無効にする方法の詳細を追加。	回避策	最終版	2018年12月4日
1.0	初回公開リリース		最終版	2018年11月28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。