# Cisco Prime Collaboration プロビジョニングは SQL インジェクション脆弱性を認証しました

High

**アドバイザリーID :** cisco-sa-20171101-cpcp

**初公開日 :** 2017-11-01 16:00

**バージョン 1.0 :** Final

**CVSSスコア :** 8.1

**回避策 :** No workarounds available

**Cisco バグ ID :** CSCvf47935

CVE-2017-12276

**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 プロビジョニング アプリケーションの SQL データベースインターフェイスのための Web フレームワーク コードの脆弱性は任意 SQL クエリの実行によってアプリケーションの機密保持および統合に影響を与える認証される、リモート攻撃者を可能にする可能性があります。 攻撃者は SQL データベースからの read または write 情報できました。

脆弱性は SQL クエリ内のユーザが指定する入力の適切な検証の欠如が原因です。 攻撃者は影響を受けたアプリケーションに悪意のある SQL 文が含まれている巧妙に細工された URL の送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者がある特定の値の存在を判別し、SQL データベースに悪意のある入力を書くことを可能にする可能性があります。 攻撃者は有効 な ユーザ 資格情報がある必要があります。

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。
101-cpcp

## 該当製品

### 脆弱性のある製品

この脆弱性は 12.3 前に Cisco Prime Collaboration プロビジョニング ソフトウェア リリースに該当します。

管理者は Cisco Prime Collaboration プロビジョニング ソフトウェアのどのリリースが **http か**を使用して Web ユーザ ユーザー・ インターフェースにログオンによって動作しているか判別できます : **//system IP** アクセス URL。 この例では、アプリケーションの Cisco Prime Collaboration プロビジョニング ソフトウェア リリース 10.6 はインストールされています。

```
Prime Collaboration
Provisioning
```

Version **10.6**管理者はまた CLI で **show version コマンドを**使用できます。 この例では、Cisco Prime Collaboration プロビジョニング ソフトウェア リリース 10.6.0.1015 はデバイスでインストールされています:

```
cpcpserver/admin# show version

Cisco Application Deployment Engine OS Release:

ADE-OS Build Version:
ADE-OS System Architecture: x86_64
Copyright (c) 2005-2017 by Cisco Systems, Inc.
All rights reserved.
Hostname: cpcpserver

Version information of installed applications
- - - - - - - - - - - - - - - - - - - - - - - - - -

Collaboration Manager
- - - - - - - - - - - - - - - - - - - - - - - - - -
Version : 10.6.0.1015
.
.
.
```

# 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。

Cisco はこの脆弱性が Cisco Prime Collaboration 保証に影響を与えないことを確認しました。

## 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。
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**

この脆弱性は Cisco Prime Collaboration プロビジョニング ソフトウェア リリース 12.3 で解決されます。

ソフトウェアは Cisco.com の Software Center から**製品 > クラウドおよびシステム管理 > 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 > Prime Collaboration** 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

Cisco はこの脆弱性を発見することおよび報告するために NATO 通信からのヴィンチェンツォ Hutsebaut および情報調査所に感謝することを望みます。

## URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-cpcp

## 改訂履歴

| Version | Description | Section | Status | 日付 |
|---|---|---|---|---|
| 1.0 | 初回公開リリース | | Final | 2017-November-01 |

## 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。