# Cisco Policy Suite for Mobile および Cisco Policy Suite 直径ルーティング エージェントソフトウェア Redis サーバ 非認証アクセス脆弱性

| | | |
|---|---|---|
| Medium | **アドバイザリーID :** cisco-sa-20190109-cps-redis<br>**初公開日 :** 2019-01-09 16:00<br>**バージョン 1.0 :** Final<br>**CVSSスコア :** 7.3<br>**回避策 :** No workarounds available<br>**Cisco バグ ID :** CSCvf08748 CSCvk64527 | CVE-2018-0181 |

**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 Policy Suite for Mobile および Cisco Policy Suite 直径ルーティング エージェントソフトウェアによって使用された Redis 実装の脆弱性はリモート攻撃者非認証が Redis サーバによって保存された短命のイベントのためのキーと値のペアを修正するようにする可能性があります。

脆弱性は Redis サーバにアクセスするとき不適当な認証が原因です。 非認証攻撃者は Redis サーバデータベースの内で保存されたキーと値のペアの修正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 Cisco Policy Suite for Mobile および Cisco Policy Suite 直径ルーティング エージェントソフトウェアの効率を減らすことを可能にする可能性があります。

Cisco は Cisco Policy Suite for Mobile のための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。

現在 Cisco Policy Suite 直径ルーティング エージェントソフトウェアのために利用可能 な ソフトウェア リリースがありません。 この脆弱性に対処する、Cisco Policy Suite 直径ルーティング エージェントソフトウェア 存在のための軽減がありません回避策。 回避策 セクションを詳細については参照して下さい。

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-20190109-cps-redis

# 該当製品

## 脆弱性のある製品

この脆弱性は脆弱 な ソフトウェア バージョンを実行する以下のシスコ製品に影響を及ぼします:

- Cisco Policy Suite for Mobile
- Cisco Policy Suite 直径ルーティング エージェント

該当するソフトウェア リリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

## 脆弱性を含んでいないことが確認された製品

シスコは、この脆弱性が以下の製品には影響を与えないことを確認しました。

- Cisco Policy Suite for BNG
- Cisco Policy Suite for Wi-Fi

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。

# 回避策

この脆弱性に対処する回避策はありません。

インターフェイスに直面する外部にアクセスのブロックによって攻撃サーフェイスを減らす Cisco Policy Suite 直径ルーティング エージェントソフトウェア 存在のための軽減。 このプロシージャはいくつかのステップが完了するように要求します。 実装の詳細および支援に関しては Cisco Technical Assistance Center （ TAC ）に連絡して下さい。

# 修正済みソフトウェア

修正済みソフトウェアリリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

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。

## 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-20190109-cps-redis

## 改訂履歴

| バージョン | 説明 | セクション | ステータス | Date |
|---|---|---|---|---|
| 1.0 | 初回公開リリース | | 最終版 | 2019-January-09 |

## 利用規約