# Cisco データセンター アナリティクス フレームワーク クロスサイト要求偽作脆弱性

| | | |
|---|---|---|
| Medium | **アドバイザリーID :** Cisco-SA-20150622-CVE-2015-4189<br>**初公開日 :** 2015-06-22 21:00<br>**バージョン 1.0 :** Final<br>**CVSSスコア :** 4.3<br>**回避策 :** No Workarounds available<br>**Cisco バグ ID :** CSCun26807 | CVE-2015-4189 |

**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

データセンター アナリティクス フレームワーク（DCAF）アプリケーションの脆弱性はリモート攻撃者非認証が不必要な操作を実行するようにする可能性があります。

脆弱性は不十分なクロスサイト要求偽作（CSRF）保護が原因です。 攻撃者は不都合なアクションの実行に Webアプリケーションのユーザのトリックによってこの脆弱性を不正利用する可能性があります。

Cisco は脆弱性を確認しました; ただし、ソフトウェア アップデートは利用できません。

この脆弱性を不正利用するために、攻撃者は、悪意のあるサイトにユーザを誘導するためのリンクを提供したり、誤解させる言葉や指示を使用して、提供されたリンクに進むようにユーザを促す可能性があります。

Cisco は CVSS スコアを通してその機能エクスプロイト コード存在を示します; ただし、コードは共用利用可能であると知られていません。

## 該当製品

Cisco は影響を受けた製品バージョンの追加詳細および最新リストが含まれている登録ユーザ向けのバグID CSCun26807 をリリースしました。

## 脆弱性のある製品

このアラートが最初に送達された時、Cisco DCAF リリース 1.4 は脆弱でした。 Cisco DCAF

の以降のリリースはまた脆弱かもしれません。

## 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

管理者は今後のアップデートおよびリリースに関するベンダーに連絡するように助言されます。

ユーザは非請求リンクが続いてが安全であることを確認する必要があります。

クロスサイト要求偽作不正侵入および潜在的な軽減方式についてのその他の情報に関しては、Cisco によって加えられる軽減情報 知識クロスサイトが偽作脅威ベクターを要求するのを参照して下さい。

管理者は影響を受けたシステムを監視するように助言されます。

### 修正済みソフトウェア

ソフトウェア アップデートは利用できません。

### 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

### URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20150622-CVE-2015-4189

### 改訂履歴

| Version | Description | Section | Status | 日付 |
|---|---|---|---|---|
| 1.0 | 初版リリース | 該当なし | Final | 2015-Jun-22 |

### 利用規約

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。