# Cisco Cloud Portalの認証されていないファイルダウンロードの脆弱性

| | | |
|---|---|---|
| Medium | **アドバイザリーID :** Cisco-SA-20131209-CVE-2013-6708<br>**初公開日 :** 2013-12-09 20:48<br>**バージョン 1.0 :** Final<br>**CVSSスコア :** 5.0<br>**回避策 :** No Workarounds available<br>**Cisco バグ ID :** CSCui60889 CSCuj08426 | CVE-2013-6708 |

**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 Cloud PortalのWeb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脆弱性のあるサーバから特定のファイルタイプをダウンロードできる可能性があります。

この脆弱性は、特定のファイルタイプに対するアクセス制御の不十分な適用に起因します。攻撃者は、ブラウザを使用して許可されたタイプのファイルをダウンロードすることにより、この脆弱性を不正利用する可能性があります。

シスコはセキュリティ通知で脆弱性を確認しましたが、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には、攻撃者がターゲットデバイスが存在する可能性のある信頼できる内部ネットワークにアクセスする必要がある可能性があります。このアクセス要件により、不正利用が成功する可能性が低くなります。

## 該当製品

該当する製品バージョンの最も完全なリストについては、Cisco Bug ID CSCuj08426およびCSCui60889を参照してください。

### 脆弱性のある製品

このアラートが最初に公開された時点では、Cisco Cloud Portal 9.4には脆弱性が存在します。Cisco Cloud Portalの新しいリリースにも脆弱性が存在する可能性があります。

### 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

今後のアップデートやリリースについては、ベンダーに連絡することを推奨します。

信頼できるユーザだけにネットワークアクセスを許可することを推奨します。

IPベースのアクセスコントロールリスト(ACL)を使用して、信頼できるシステムだけに該当システムへのアクセスを許可することを検討することもできます。

影響を受けるシステムを監視することを推奨します。

## 修正済みソフトウェア

ソフトウェアの更新プログラムは利用できません。

## 不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20131209-CVE-2013-6708

## 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 | 初版リリース | 適用外 | Final | 2013年12月9日 |

## 利用規約

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。