Cisco Prime Central for HCSポータルのクレデンシャルアクセスの脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20131010-CVE-2013-3409 **初公開日 :** 2013-10-10 17:45 **バージョン 1.0 :** Final **CVSSスコア :** 4.3 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCuh34230 CSCuh33735	CVE-2013-3409

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 Central for HCSポータルの脆弱性により、認証されたローカルの攻撃者がアカウントのクレデンシャルを取得できる可能性があります。

この脆弱性は、不適切な権限を持つ一時ファイルへのクレデンシャルのプレーンテキストロギングに起因します。攻撃者は、ファイルにアクセスしてクレデンシャルを取得し、それを使用してデータベースなどの内部アプリケーションコンポーネントにアクセスすることで、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。

攻撃者は、認証を行い、ターゲットデバイスへのローカルアクセスを持つ必要があります。このアクセス要件により、攻撃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 CSCuh33735およびCSCuh34230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 Prime Central for HCSバージョン9.2.1以前には脆弱性が存在していました。Cisco Prime Central for HCS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。

信頼できるユーザだけがローカルシステムにアクセスできるようにすることを推奨します。

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-20131010-CVE-2013-3409

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10月10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。

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。