Cisco Prime Infrastructureデバイスディスカバリパスワード漏えいの脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20141222-CVE-2014-8007 **初公開日 :** 2014-12-22 17:39 **バージョン 1.0 :** Final **CVSSスコア :** 4.0 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCum00019	CVE-2014-8007

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 InfrastructureのWebインターフェイスの脆弱性により、認証されたリモートの攻撃者がデバイス検出用に保存されたパスワードを表示できる可能性があります。

この脆弱性は、Quick Discoveryオプションページに HMTLページソースに保存されたパスワードが含まれているために発生します。攻撃者は、ページのHTMLソースを調べることにより、この脆弱性を不正利用する可能性があります。

この脆弱性を不正利用するプルーフオブコンセプトコードは一般に公開されています。

シスコは脆弱性を確認し、更新されたソフトウェアをリリースしました。

この脆弱性を不正利用するには、攻撃者は該当デバイスへの認証アクセスを持っている必要があります。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

シスコは次のリンクでセキュリティアドバイザリをリリースしました： CVE-2014-8007

脆弱性のある製品

Cisco Prime Infrastructureバージョン2.0.0には脆弱性が存在します。

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

適切なアップデートを適用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

シスコのお客様は、更新されたソフトウェアについて通常のシスコサポートチャネルに問い合わせることをお勧めします。

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-20141222-CVE-2014-8007

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	2014年12月22日

利用規約

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。