Cisco Unified Computing Systemファブリックインターコネクトにおけるcreate certreqコマンド注入の脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20131003-CVE-2012-4111 **初公開日 :** 2013-10-03 12:40 **バージョン 1.0 :** Final **CVSSスコア :** 6.8 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCtq86563	CVE-2012-4111

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 Unified Computing System(UCS)ファブリックインターコネクトの **create certreq**コマンドの脆弱性により、認証されたローカルの攻撃者がコマンドを実行し、 *root*ユーザとしてインタラクティブなLinuxシェルを取得する可能性があります。

この脆弱性は、ユーザ入力を適切にサニタイズできないことに起因します。攻撃者は、一般的な手法を使用してLinuxシェルコマンドをパラメータに挿入することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はLinuxシェルで *root*ユーザとして任意のコマンドを実行できる可能性があります。攻撃者は、 *root*ユーザとしてインタラクティブなLinuxシェルを取得することで、基盤となるオペレーティングシステムへの完全なアクセス権を取得することもできます。

シスコは、セキュリティ通知で脆弱性を確認し、ソフトウェアアップデートをリリースしました。

この脆弱性を不正利用するには、攻撃者はターゲットシステムへの認証されたアクセスを必要とします。認証されたアクセスでは、攻撃者は信頼できる内部ネットワークにアクセスする必要があります。これらのアクセス要件により、不正利用が成功する可能性が制限される可能性があります。

シスコはCVSSスコアを通じて、機能不正利用コードが存在することを示していますが、このコードが一般に公開されているかどうかは不明です。

該当製品

影響を受ける製品バージョンの完全なリストについては、Cisco Bug ID CSCtq86563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 Unified Computing Systemバージョン2.1以前には脆弱性が存在していました。Cisco Unified Computing System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

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。

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。

管理者は、特権を持つユーザだけに管理システムまたは管理システムへの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

有効な契約を結んでいるシスコのお客様は、 CiscoのSoftware Centerからアップデートを入手できます。契約を結んでいないシスコのお客様は、Cisco Technical Assistance Center(TAC)に1-800-553-2447または1-408-526-7209で連絡するか、 *tac@cisco.com*で電子メールを介してアップグレードを入手できます

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-20131003-CVE-2012-4111

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3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。