

Cisco Nexus 1000Vライセンスインストールコマンドインジェクションの脆弱性

Medium	アドバイザーID : Cisco-SA-20130709-CVE-2013-3400	CVE-2013-3400
	初公開日 : 2013-07-09 21:36	
	バージョン 1.0 : Final	
	CVSSスコア : 6.6	
	回避策 : No Workarounds available	
	Cisco バグ ID : CSCuh30824	

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 Nexus 1000Vのライセンスインストールモジュールの脆弱性により、認証されたローカルの攻撃者が任意のシェルコマンドを実行できる可能性があります。

この脆弱性は、`install license`コマンドがユーザ指定の入力を正しく検証できないことに起因します。攻撃者は、`install license`コマンドに巧妙に細工された引数を提供することにより、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、ソフトウェアアップデートをリリースしました。

デバイスにアクセスし、脆弱性のあるコマンドを実行するために十分な権限で認証を行えるユーザだけが、この脆弱性を不正利用する可能性があります。アクセス要件により、潜在的な攻撃の発信元が大幅に制限されます。

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 [CSCuh30824](#)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 NX-OSソフトウェアバージョン4.2は、Cisco Nexus 1000Vデバイス上で動作している場合に脆弱性が存在していました。Cisco NX-OSソフトウェアの他のバージョンも影響を受け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

アップデートが利用可能になった時点で適用することをお勧めします。

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。

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-20130709-CVE-2013-3400>

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7月9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、単独の転載や意識を施した場合、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。