Cisco NexusデバイスのPythonサブシステムローカル権限昇格の脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20150630-CVE-2015-4234 **初公開日 :** 2015-06-30 22:03 **バージョン 1.0 :** Final **CVSSスコア :** 6.8 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCur00127 CSCur00115 CSCun02887	CVE-2015-4234

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 NX-OSソフトウェアを実行しているCisco NexusデバイスのPythonサブシステムに複数の権限昇格の脆弱性が存在するため、認証されたローカルの攻撃者が昇格された権限を取得する可能性があります。

この脆弱性は、NX-OSの基盤となるオペレーティングシステムが十分に強化されていないことに起因します。該当デバイスで任意のPythonスクリプトを実行するのに十分な権限を持つ攻撃者は、このアクセス権を使用して *ルート*権限を取得する可能性があります。

シスコは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。

これらの脆弱性をエクスプロイトするには、攻撃者がローカルアクセスを持ち、ターゲットデバイスに対して認証を行う必要があります。これらの要件により、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。

この脆弱性を発見し、報告していただいたJens Krabbenhoeft氏に感謝いたします。

該当製品

シスコは、登録ユーザ向けにBug ID CSCun02887、 CSCur00115、および CSCur00127をリリースしました。これらのBug IDには、追加情報と、影響を受ける製品バージョンの最新リストが含まれています。

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ソフトウェアリリース6.0(2)および6.2(2)を実行しているCisco Nexusデバイスには脆弱性が存在していました。Cisco NX-OSソフトウェア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。

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-20150630-CVE-2015-4234

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	2015年6月30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。