Cisco Webセキュリティアプライアンスの Pythonファイル処理における特権昇格の脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20150413-CVE-2015-0693 **初公開日 :** 2015-04-13 16:21 **バージョン 1.0 :** Final **CVSSスコア :** 6.6 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2015-0693

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 Webセキュリティアプライアンス(WSA)をサポートするためのリモートアクセストンネルのステータスチェックプロセスにおける脆弱性により、認証されたローカルの攻撃者が、該当システムで任意のPythonコードを実行する可能性があります。

この脆弱性は、該当ソフトウェアによる **pickle** Pythonモジュールの不適切な使用と処理に起因します。攻撃者は、巧妙に細工されたpickleファイルを該当デバイスに送信することで、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、さらなる攻撃に利用される可能性があります。

シスコはこの脆弱性を確認していますが、利用可能なソフトウェアアップデートはありません。

この脆弱性をエクスプロイトするには、攻撃者は脆弱なデバイスにローカルでログインする必要があります。このアクセス要件により、不正利用の可能性が低減されます。

該当製品

シスコは、登録ユーザ向けにバグID CSCut39259をリリースしました。このバグには、影響を受ける製品バージョンの詳細と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 WSAソフトウェアバージョン8.5.0-ise-147に脆弱性が存在していました。Cisco WSA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、適切なアップデートを適用することをお勧めします。

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-20150413-CVE-2015-0693

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4月13日

利用規約

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。