Cisco ASAローカルパス包含の脆弱性

Medium

アドバイザリーID : Cisco-SA-20141008-CVE-2014-3391　CVE-2014-3391
初公開日 : 2014-10-08 16:09
バージョン 1.0 : Final
CVSSスコア : 6.8
回避策 : No Workarounds available
Cisco バグ ID : CSCtq52661

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 ASAソフトウェアの環境変数をエクスポートする機能の脆弱性により、認証されたローカルの攻撃者が悪意のあるライブラリを挿入し、システムを完全に制御できる可能性があります。

この脆弱性は、LD_LIBRARY_PATH環境の不適切な設定に起因します。攻撃者は、悪意のあるライブラリを該当システムの外部メモリにコピーし、システムのリロードをトリガーすることで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は該当システムに悪意のあるライブラリをロードさせ、基盤となるLinux OSにアクセスさせ、システムの完全な侵害を引き起こす可能性があります。

シスコはセキュリティアドバイザリでこの脆弱性を確認し、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。

本脆弱性を不正利用する目的で使用できるのは、該当システム宛てのトラフィックに限られます。この脆弱性は、シングルおよびマルチコンテキストモードの両方で、ルーテッドファイアウォールモードとトランスペアレントファイアウォールモードの両方に影響します。この脆弱性を不正利用するには、システムのリロードが必要です。デフォルト設定では、この脆弱性をエクスプロイトするには、 Administrationまたは privilege 15のアクセス権が必要です。

シスコはCVSSスコアを通じて、機能的なエクスプロイト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ることは確認されていません。

該当製品

シスコは、次のリンクでBug ID CSCtq52661のセキュリティアドバイザリをリリースしています。 cisco-sa-20141008-asa

脆弱性のある製品

シスコはセキュリティアドバイザリで、影響を受けるCisco適応型セキュリティアプライアンス(ASA)ソフトウェアリリースのリストを公開しています。このアラートの「Vendor Announcements」セクションには、アドバイザリへのリンクが含まれています。

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。

信頼できるユーザー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、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、管理者ユーザーのみが管理システムまたは管理システムにアクセスすることを許可することを推奨します。

管理者は、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が該当システムにアクセスできるようにすることを検討できます。

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

契約が有効なシスコのお客様は、 CiscoのSoftware Centerからアップデートを入手できます。契約をご利用でないお客様は、1-800-553-2447または1-408-526-7209のCisco Technical Assistance Center(TAC)にお問い合わせいただくか、 tac@cisco.comのEメールでアップグレードを入手できます。

推奨事項

$propertyAndFields.get("recommendations")

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-20141008-CVE-2014-3391

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10月8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。