Cisco Access Control Serverのクロスサイトスクリプティングの脆弱性

アドバイザリーID : Cisco-SA-20150513-CVE-2015-0728
初公開日 : 2015-05-13 17:10
バージョン 1.0 : Final
CVSSスコア : 4.3
回避策 : No Workarounds available
Cisco バグ ID : CSCuu11002

CVE-2015-0728

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 Access Control Server(ACS)の脆弱性により、認証されていないリモートの攻撃者がクロスサイトスクリプティング(XSS)攻撃を実行する可能性があります。

この脆弱性は、該当デバイスに渡された特定のパラメータの入力検証が不適切なことに起因します。攻撃者は、悪意のあるリンクにアクセスするようユーザを誘導することで、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、攻撃者は該当サイトに関連する任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセスしたりす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、ソフトウェアアップデートは提供されていません。

この脆弱性を不正利用するために、攻撃者は悪意のあるサイトにユーザを誘導するリンクを提供し、誤解を招く言語または指示を使用してユーザをリンクに従わせることがあります。

該当製品

シスコは登録ユーザ向けにBug ID CSCuu11002をリリースしました。このIDには、詳細情報と、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 ACSバージョン5.5(0.1)に脆弱性が存在していました。Cisco ACSの新しいバージョン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、ベンダーに問い合わせることをお勧めします。

ユーザは、非要請リンクが安全に追跡できることを確認する必要があります。

XSS攻撃およびこの脆弱性を悪用するために使用される方法の詳細については、Cisco適用対応策速報『 クロスサイトスクリプティング(XSS)の脅威ベクトルについて』を参照してください。

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。

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-20150513-CVE-2015-0728

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5月13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。