CiscoワイヤレスLANコントローラのHTMLヘルプにおけるクロスサイトスクリプティングの脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20150406-CVE-2015-0690 **初公開日 :** 2015-04-06 17:30 **バージョン 1.0 :** Final **CVSSスコア :** 4.3 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2015-0690

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ワイヤレスLANコントローラ(WLC)デバイスのHTMLヘルプシステムの脆弱性により、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攻撃を実行する可能性があります。

認証されていないリモートの攻撃者が、該当システムのユーザを説得して悪意のあるリンクにアクセスさせたり、攻撃者によって制御されるWebページにアクセスさせたりすると、該当サイトのセキュリティコンテキストで任意のHTMLまたはスクリプトコードを実行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ためのリンクを提供したり、誤解させる言葉や指示を使用して、提供されたリンクに進むようにユーザを促す可能性があります。

シスコはCVSSスコアを通じて、機能不正利用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ているかどうかは不明です。

該当製品

シスコは、登録ユーザ向けにバグID CSCun95178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

8.0より前のバージョンのWLCソフトウェアを実行しているCisco WLCデバイスが影響を受けます。

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。

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攻撃と、これら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』の「 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。

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-20150406-CVE-2015-0690

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6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。