Cisco FireSIGHT Management Centerの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-20150608-CVE-2015-0737 CVE-2015-0737
初公開日 : 2015-06-08 21:52
最終更新日 : 2015-07-07 13:10
バージョン 4.0 : Final
CVSSスコア : 3.5
回避策 : No Workarounds available
Cisco バグ ID : CSCuu91342 CSCuu11099 CSCuu91326

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 FireSIGHT Management Centerの脆弱性により、認証されたリモートの攻撃者がクロスサイトスクリプティング(XSS)攻撃を実行できる可能性があります。

この脆弱性は、HTTP GETまたはPOSTメソッドを介して渡される一部のパラメータの入力検証が不十分であることに起因します。攻撃者は、ユーザパケットを傍受し、悪意のあるコードを挿入することで、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、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、ブラウザの機密情報にアクセスしたりでき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。

シスコは、この脆弱性を報告したCheck Point Security Research TeamのLiad Mizrachi氏とOded Vanunu氏の功績を称えたいと考えています。

該当製品

シスコは登録ユーザ向けにバグID CSCuu11099 、CSCuu91342、およびCSCuu91326をリリースしました。これらのバグには、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 FireSIGHTシステムソフトウェアバージョン5.3.1.1に脆弱性が存在していました。Cisco FireSIGHTシステムソフトウェア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-20150608-CVE-2015-0737

改訂履歴

バージョン	説明	セクション	ステータス	日付
3.0	IntelliShieldはこのアラートを更新し、影響を受けるバージョンと、Cisco FireSIGHT Management Centerのクロスサイトスクリプティングの脆弱性に関連する情報を追加しました。	適用外	Final	2015年6月30日
2.0	IntelliShieldはこのアラートを更新し、Cisco FireSIGHT Management Centerのクロスサイトスクリプティングの脆弱性に関連する情報を修正しました。	適用外	Final	2015年6月25日
1.0	Cisco FireSIGHT Management Centerには、認証されていないリモートの攻撃者によるクロスサイトスクリプティング攻撃を可能にする脆弱性が存在します。更新プログラムは利用できません。	適用外	Final	2015年6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。