Cisco FireSIGHT Management Center Web フレームワークによって保存されるクロスサイト スクリプティング脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20150422-CVE-2015-0707 **初公開日 :** 2015-04-22 20:33 **最終更新日 :** 2015-06-18 12:50 **バージョン 5.0 :** Final **CVSSスコア :** 3.5 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCut47196 CSCus85425 CSCus93566 CSCur58911 CSCuu68205 CSCut31557	CVE-2015-0707

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 （ MC ）の Web フレームワークの脆弱性は Webインターフェイスのユーザに対して保存されたクロスサイト スクリプティング（ XSS ）不正侵入を実行する認証される、リモート攻撃者可能にする可能性があります。

脆弱性はパラメータ値の不適当な sanitization が原因です。 攻撃者は悪意のあるコードを影響を受けたパラメータにインジェクトし、読み取りかパラメータを実行することを必要とする Webページにアクセスするようにユーザを確信させることによってこの脆弱性を不正利用する可能性があります。

Cisco は脆弱性およびリリースされたソフトウェア アップデートを確認しました。

脆弱性を不正利用するために、攻撃者は影響を受けたアプリケーションのパラメータに悪意のあるコードをインジェクトする許可されたアクセスをアクセスできなければなりません。 このアクセス要件は正常なエクスプロイトの確率を減少させるかもしれません。

攻撃者はユーザをリンクに従うように説得する悪意のあるサイトおよび使用紛らわしい言語または手順にターゲットとされたユーザを指示するリンクを提供するかもしれません。

Cisco はこの脆弱性を報告するためにまたは Moran、Lior Neumann、Liad Mizrachi、および点検点 セキュリティ研究チームからの Oded Vanunu 感謝することを望みます。

該当製品

Cisco は影響を受けた製品バージョンの追加詳細および最新リストが含まれている登録ユーザ向けのバグID CSCus85425、 CSCus93566、CSCut31557、CSCut47196、CSCur58911、CSCuu68205 および CSCus04436 をリリースしました。

脆弱性のある製品

このアラートが最初に送達された時、Cisco SireSIGHT システムソフトウェアバージョン 5.3.1.1 および 6.0.0 は脆弱でした。 Cisco SireSIGHT システム ソフトウェアの以降のバージョンはまた脆弱かもしれません。

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

管理者は適切な更新を加えるように助言されます。

ユーザは非請求リンクが続いてが安全であることを確認する必要があります。

XSS 不正侵入およびこれらの脆弱性を不正利用するのに使用される方式についてのその他の情報に関しては Cisco によって加えられる軽減情報 知識クロスサイト スクリプティング 脅威ベクターを参照して下さい。

管理者は影響を受けたシステムを監視するように助言されます。

修正済みソフトウェア

アクティブな契約を持つ Cisco カスタマは次のリンクで Software Center を通して更新を入手できます: Cisco。 契約のない Cisco カスタマは 1-800-553-2447 か 1-408-526-7209 でまたは *tac@cisco.com* でメールで Cisco Technical Assistance Center にコンタクトをとってアップグレードを入手できます。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20150422-CVE-2015-0707

改訂履歴

Version	Description	Section	Status	日付
4.0	IntelliShield は Cisco FireSIGHT Management Center Web フレームワークによって保存されるクロスサイト スクリプティング脆弱性に関してその他の情報を含むためにこのアラートをアップデートしました。	該当なし	Final	2015-Jun-16
3.0	IntelliShield は Cisco FireSIGHT Management Center Web フレームワークによって保存されるクロスサイト スクリプティング脆弱性に関して影響を受けたソフトウェア リリースおよびその他の情報を追加するためにこのアラートをアップデートしました。	該当なし	Final	2015-Jun-08
2.0	IntelliShield は Cisco FireSIGHT Management Center Web フレームワークによって保存されるクロスサイト スクリプティング脆弱性に関してその他の情報を追加するためにこのアラートをアップデートしました。	該当なし	Final	2015-Jun-03
1.0	Cisco FireSIGHT Management Center は認証される可能にする可能性がある保存されたクロスサイト スクリプティング攻撃を行なうために脆弱性がリモート攻撃者含まれています。 更新は利用できます。	該当なし	Final	2015-Apr-22

利用規約