Cisco AsyncOS ISQ XSSの脆弱性

アドバイザリーID : Cisco-SA-20150114-CVE-2015-0577 CVE-2015-0577
初公開日 : 2015-01-14 18:54
バージョン 1.0 : Final
CVSSスコア : 4.3
回避策 : No workarounds available
Cisco バグ ID : CSCup08113 CSCus22925

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 AsyncOSのWebフレームワークの脆弱性により、認証されていないリモートの攻撃者が該当システムのWebインターフェイスのユーザに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、IronPortスパム検疫Webページの複数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、悪意のあるリンクにアクセスするように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。

シスコはセキュリティ通知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、誤解を招く言語や指示を使用してユーザがリンクに従うように説得する可能性があります。

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唆していますが、このコードが一般に公開されているとは認識していません。

該当製品

脆弱性のある製品

次のシスコ製品で実行されているCisco AsyncOSソフトウェアが影響を受けます。

- Cisco Eメールセキュリティアプライアンスバージョン7.1、7.3、7.5、7.6、7.8
- Ciscoコンテンツセキュリティ管理アプライアンスバージョン7.2、7.7、7.8、7.9、8.0、8.1

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と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、非要請リンクを安全に追跡できることを確認する必要があります。

影響を受けるシステムをモニタすることをお勧めします。

修正済みソフトウェア

有効な契約をご利用のシスコのお客様は、Software Center(Cisco)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、Cisco Technical Assistance Center(TAC)に1-800-553-2447または1-408-526-7209で連絡するか、 tac@cisco.comから電子メールで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）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-20150114-CVE-2015-0577

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1月14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。