

Cisco Router and Security Device Manager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-20100429- [CVE-2010-0594](#)
CVE-2010-0594
初公開日 : 2010-04-29 18:32
バージョン 1.0 : Final
CVSSスコア : [4.3](#)
回避策 : No Workarounds available
Cisco バグ ID :

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 Router and Security Device Manager(SDM)バージョン2.5以前には、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。

この脆弱性は、アプリケーションによって処理されるパラメータの検証が不適切なことに起因します。認証されていないリモートの攻撃者は、この脆弱性を不正利用して、悪意のあるURLにアクセスするようユーザを誘導する可能性があります。成功すると、攻撃者はユーザのブラウザセッションで任意のスクリプトまたはHTMLコードを実行する可能性があります。

シスコはバグエントリの脆弱性を確認しましたが、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には、攻撃者は提供されたURLに従うようにユーザを誘導する必要があります。攻撃者は、電子メールメッセージ内でURLをユーザに送信するか、Webサイトに掲載する可能性があります。攻撃者は、ソーシャルエンジニアリング技術を使用して、提供されたリンクを信頼するようユーザを誘導する可能性があります。

アプリケーションへのアクセス権を持つユーザだけがエクスプロイトに参加できます。アプリケーションの性質上、管理タスクを実行するユーザが必要なアクセス権を持つことはほとんどなく、悪用の可能性は限られています。

Cisco RouterおよびSecurity Device Managerの修正プログラムは利用できませんが、Cisco Configuration Professionalはそのまま導入できます。このソフトウェアは、[Cisco Configuration Professional](#)

該当製品

シスコは次のリンクでバグエントリをリリースしました。 [CSCtb38467](#)

JPCERTは次のリンクで脆弱性に関するノートを公開しました。 [14313132](#)

脆弱性のある製品

Cisco Router and Security Device Managerバージョン2.5以前には脆弱性が存在します。

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用することを推奨します。

管理者は、信頼できるユーザだけにアプリケーションアクセスを許可することを推奨します。

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。

アプリケーションを使用していないときは、アプリケーションからログアウトすることをお勧めします。

管理者は重要な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

パッチおよびソフトウェアアップデートは利用できません。

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-20100429-CVE-2010-0594>

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	2010年4月29日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、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。