

Cisco ASAソフトウェアWebVPN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-20090401- [CVE-2009-1220](#)
CVE-2009-1220
初公開日 : 2009-04-01 15:41
最終更新日 : 2012-07-14 15:20
バージョン 3.0 : 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 ASAソフトウェアバージョン8.0.4(28)以前には、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。

この脆弱性は、WebVPNのクライアントレスモード機能での不十分な入力検証に起因します。攻撃者は、この脆弱性を不正利用してクロスサイトスクリプティング攻撃を実行し、サイトのセキュリティコンテキスト内のユーザのブラウザセッションで任意の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。

このクロスサイトスクリプティング攻撃を実証するプルーフオブコンセプトコードを利用できません。

シスコは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には、WebVPN機能のクライアントレスモードを有効にする必要があります。攻撃者は、巧妙に細工されたHTTPヘッダーをブラウザに挿入する必要があります。これには、JavaScriptやFlashなどのWebアプリケーションテクノロジーを使用する必要があります。これらの要因により、攻撃の可能性が低下します。

この不正利用により、攻撃者はWebVPNセッションCookieを取得し、VPNデバイスへの不正アクセスを取得できる可能性があります。

該当製品

シスコは、Cisco Bug ID [CSCsy82093](#)でこの脆弱性を確認しています。シスコは、該当ソフトウェアの修正済みバージョンを含むようにこのバグIDを更新しました。

脆弱性のある製品

Cisco ASA 5500シリーズ適応型セキュリティアプライアンスを実行しているCisco ASAソフトウェアバージョン8.0.4(28)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

適切なアップデートを適用することを推奨します。

影響を受けるシステムへのアクセスを信頼できるユーザに制限することを推奨します。

未承諾のリンクは使用しないことをお勧めします。ユーザは、予期しないリンクを追跡する前に、その信頼性を確認する必要があります。

修正済みソフトウェア

契約が有効なシスコのお客様は、[Cisco](#)のSoftware Center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、1-800-553-2447または1-408-526-7209のCisco Technical Assistance Center(TAC)に連絡するか、tac@cisco.comのEメールでアップグレードを入手できます。

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-20090401-CVE-2009-1220>

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	2009年4月1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。