

Cisco Router and Security Device Manager 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-20100429-CVE-2010-0594	CVE-2010-0594
m	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 : Yes	
	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 バージョン 2.5 は前に攻撃者がクロスサイト スクリプティング攻撃を行なうことを可能にする可能性がある脆弱性が含まれ。

アプリケーションによって処理されるパラメータの不適切な検証による脆弱性存在。非認証はユーザの悪意のある URL に続くように確信によって、リモート攻撃者脆弱性を不正利用する可能性があります。成功すれば、攻撃者はユーザのブラウザ セッションの任意スクリプトが HTML コードを実行する可能性があります。

Cisco は不具合 エントリの脆弱性を確認しました; ただし、更新は利用できません。

この脆弱性を不正利用するために、攻撃者はユーザを提供された URL に続くように確信させる必要があります。攻撃者はユーザに Webサイトで URL を電子メール メッセージ内のまたは掲示される送信 するかもしれません。攻撃者はユーザを提供されたリンクを信頼するように確信させるために社会工学手法を使用するかもしれません。

アプリケーションへのアクセスのユーザだけエクスプロイトに加わることができます。非常に管理 タスクを行う少数のユーザは不正利用のための可能性を制限する必須アクセスがあるアプリケーションの性質が原因で、可能性が高いといえます。

Cisco Router and Security Device Manager のための修正が利用できないが、ユーザは代わりに Cisco Configuration Professional を展開できます。ソフトウェアは次のリンクで利用できます:
[Cisco Configuration Professional](#)

該当製品

修正済みソフトウェア

Cisco Router and Security Device Manager バージョン 2.5 は前に脆弱であり。

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。

改訂履歴

バージョン	説明	Section	ステータス	日付
1.0	初版リリース	該当なし	Final	2010-Apr-29

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。