脆弱性を分割する Cisco ASA ソフトウェア HTTP応答

Medium	**アドバイザリーID :** Cisco-SA-20100625-CVE-2008-7257 **初公開日 :** 2010-06-25 18:34 **バージョン 1.0 :** Final **CVSSスコア :** 4.3 **回避策 :** Yes **Cisco バグ ID :**	CVE-2008-7257

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

8.1(2) 以前の Cisco ASA ソフトウェア バージョンは非認証を可能にする可能性があるクロスサイト 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。

URL 内の文字の不適当な処理による脆弱性存在。 非認証はユーザの悪意のある URL を表示するように確信によって、リモート攻撃者この脆弱性を不正利用する可能性があります。 成功すれば、攻撃者は影響を受けたサイトのセキュリティ コンテキストのユーザーのブラウザー内の任意スクリプトを実行する可能性があります。

プルーフ オブ コンセプト コードは利用できます。

Cisco はソフトウェア リリース メモのこの脆弱性を確認し、更新済ソフトウェアをリリースしました。

脆弱性を不正利用するために、攻撃者はユーザを悪意のあるリンクを表示するように確信させる必要があります。 攻撃者はユーザに送られる電子メール メッセージ内のリンクを提供するかもしれません。 ユーザー ビューがリンク、攻撃者 Cisco ASA Webインターフェイスのセキュリティ コンテキストのユーザーのブラウザーの任意スクリプト コードを実行できれば。 エクスプロイトは攻撃者がユーザーの資格情報または最近入れられたデータのような機密情報へのアクセス権を得ることを可能にする可能性があります。

Cisco はこの脆弱性を検出するために SecureWorks からのダニエル王に感謝することを望みます。

該当製品

修正済みソフトウェア

8.1(2) 以前の Cisco ASA ソフトウェア バージョンは脆弱です。

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。

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-Jun-25

利用規約