Cisco ASA 適応性があるセキュリティ ApplianceÂ Clientless SSL VPNÂ DOM 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-20090624-CVE-2009-1201 **初公開日 :** 2009-06-24 16:08 **最終更新日 :** 2012-07-14 15:12 **バージョン 2.0 :** Final **CVSSスコア :** 4.3 **回避策 :** Yes **Cisco バグ ID :**	CVE-2009-1201

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

Clientless SSL VPN 接続を許可するために設定される 8.0.4(34)、8.1.2(25)、および 8.2.1(3) 以前の Cisco ASA 適応型セキュリティ アプライアンス（ASA）ソフトウェア ソフトウェア バージョンはクロスサイト スクリプティング脆弱性から影響を受けます。 バージョン 7.x は影響を受けていません。

脆弱性はクライアントが VPN ウェブ ポータルを使用して Webページを参照するとき Cisco ASA の SSL VPN 機能が使用する JavaScript ベースのドキュメント オブジェクト モデル（DOM）がアクセスの不十分な制限が原因です。 ユーザがセキュア ポータルにログオンされる間、非認証が、リモート攻撃者 ユーザを悪意のあるページを参照するように確信できれば、攻撃者は影響を受けたサイトのセキュリティ コンテキストの任意スクリプトか HTML コードを実行する可能性があります。

Cisco は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。

脆弱性はきちんと不正な修正から Clientless SSL VPN の DOM を保護する失敗が原因です。 脆弱性は可能性が高いです管理者がユーザがセキュア ウェブ ポータルを使用して参照される任意 URL を入力することを許可するケースで不正利用される。 ユーザが管理者によって定義された URL だけ参照することを可能にするシステムは影響を受けてまずないです。 管理者が URL を定義するとき、攻撃者はこれらの URL の 1 つに常駐する、または行います攻撃を行うために種類

の URL スプーフィングまたはハイジャックを必要があります Webサイトを管理する。

クロスサイト スクリプティング脆弱性をである共用利用可能示すコードを不正利用して下さい。

該当製品

修正済みソフトウェア

8.0.4(34)、8.1.2(25)、および 8.2.1(3) 以前の Cisco ASA ソフトウェア バージョンは ASA 5505、5510、5520、5540、5550、および 5580 のデバイスを on Cisco 実行しているとき影響を受けています。

Cisco ASA ソフトウェア バージョン 7.x は影響を受けていません。

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	2009-Jun-24

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。