Cisco ガードはクロスサイト スクリプティングをイネーブルに設定します

Low

アドバイザリーID : cisco-sa-20060920-guardxss
初公開日 : 2006-09-20 16:00
最終更新日 : 2012-01-02 12:18
バージョン 1.1 : Final
CVSSスコア : 1.9
回避策 : Yes
Cisco バグ ID :

CVE-2006-4909

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 ガードの脆弱性はガードが Webブラウザクライアントと Webサーバ間のアンチスプーフィング サービスを提供しているときクロスサイト スクリプティングの使用の悪意のある Webサイトに Webブラウザクライアントを送信 することを攻撃者が可能にするかもしれません。 攻撃者は Webブラウザクライアントに悪意のある URL を提供することによって悪意のある Webサイト、か瞬時にメッセージの続かれる電子メールでに、頻繁に入るためにこれを不正利用することができます。 この問題は保護された Webサイトが XSS を可能にしなくても発生するかもしれません。 ソフトウェアアップグレードがこの脆弱性を解決するために必要となります。 利用可能 な回避策が脆弱性の効果を軽減するためにあります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060920-guardxss で利用できます。

該当製品

修正済みソフトウェア

以下のシスコ製品は脆弱です。

- Cisco ガード アプライアンス (ソフトウェア バージョン 3.X)
- Cisco ガード ブレード (ソフトウェア バージョン 4.X)
- Cisco ガード アプライアンス[ソフトウェア バージョン 5.0(3)]
- Cisco ガード アプライアンス[ソフトウェア バージョン 5.1(5)]

脆弱性を含んでいないことが確認された製品

その他のCisco製品は脆弱であるために確認されていません。

Cisco ガード DDoS 軽減アプライアンスが動作していることソフトウェア バージョンを判別する 3 つの方法があります。 各メソッドの例はここに示されています:

- **仮想端末装置またはローカル シリアルコンソール接続**
  ソフトウェアバージョン番号をアプライアンスに接続するためにローカル シリアルコンソール 使用によって判別するためシリアルケーブルおよび終端エミュレーションプログラム。 接続されたら、ターミナルの**入力 キーを**押せばガードは、ログオンしないで、デバイスで動作するソフトウェアのバージョンを示します:
  ```
  Cisco Guard Version 3.1(0.12)

  GUARD login:
  ```
  この例で Cisco ガードはソフトウェア バージョン 3.1 を実行しています。
  仮想端末装置に関しては、プロシージャは同じです但し例外としてはシリアルケーブルか終端エミュレーションプログラムは必要ではないです（標準キーボードおよびモニタはアプライアンスに直接接続されます）。
- **遠隔セキュア シェル（SSH）結合**
  ソフトウェアバージョン番号を SSH セッションによって得、SSH クライアントを Cisco ガードにログインに使用し、**show version** Command Line Interface （ CLI ） コマンドを発行するため。
  ```
  prompt$ ssh admin@guard.example.com
  admin@guard.example.com's password:
  Last login: Wed Nov 24 22:45:53 on ttyS0
  admin@GUARD#show version
  Copyright (c) 2000-2004 Cisco Systems, Inc. All rights reserved.

  Software License Agreement

  [...]

  Cisco Anomaly Guard
  Release: 3.1(0.12)
  Date:    2004/10/27 19:58:14

  GUARD uptime is 3 weeks, 3 days, 17 hours, 53 minutes
  System Serial Number:  XXXXXXX
  ```
  この例では、Cisco トラフィック異常ガードはソフトウェアバージョン 3.1 を実行しています。
- **リモート セキュア Web セッション**
  Cisco ガードがセキュア Webインターフェイスを通して実行しているソフトウェア バージョンを得るために、Webブラウザの***監視の*** URL **https:// *IP アドレスを***、ログイン開き、次にブラウザウィンドウの右上 セクションにあるリンクを約クリックして下さい。

改訂履歴

リビジョン 1.1	2011-January-02	脆弱性記録詳細のテンプレート テキストをアップデートしました

リビジョン 1.0	2006-September-20	初回公開リリース

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。