IOS HTTPサーバ コマンド インジェクト脆弱性

High

アドバイザリーID : cisco-sa-20051201-http

初公開日 : 2005-12-01 21:00

バージョン 2.0 : Final

CVSSスコア : 7.6

回避策 : Yes

Cisco バグ ID : CSCsc64976

CVE-2005-3921

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

show buffers コマンドからの出力のような動的に生成された出力に、挿入された HTML コードがページを要求するブラウザに通じる IOS HTTPサーバで存在 する脆弱性。 この HTML コードはクライアント ブラウザによって解読され、デバイスか他の可能性のある クロスサイト スクリプティング攻撃に対して可能性としては悪意のあるコマンドを実行する可能性があります。 この脆弱性の不正利用の成功はユーザが HTML コマンドがインジェクトされた含むページ ダイナミック コンテンツをブラウズすることを必要とします。

Cisco は影響を受けた顧客向けのこの脆弱性に対処するためにフリーソフトを使用できるようにします。 この脆弱性に対しては、影響を緩和するための回避策があります。

このアドバイザリは 201-http で掲示されます。

該当製品

修正済みソフトウェア

この Security Advisory は有効に なる HTTPサーバの Cisco IOS ソフトウェア バージョン 11.0 ～ 12.4 を実行するすべてのシスコ製品に適用します。 システムに IOS HTTPサーバか HTTP セキュアサーバが含まれている、有効に なるそれが影響を受けていませんありませんが。

HTTPサーバがデバイスで動作したかどうか確認するために、**提示 ip http server ステータスを**発行し、プロンプトで **ip http server にセキュア status コマンドを示し、**に類似した出力を探して下さい:

```
Router>show ip http server status
HTTP server status: Enabled
```

デバイスが HTTPサーバを実行しない場合、に類似した出力を見るはずです:

```
Router>show ip http server status
HTTP server status: Disabled
```

下記の修正済みソフトウェアのセクションにリストされるバージョン前の Cisco IOS のどのバージョンでも脆弱かもしれません。

脆弱性を含んでいないことが確認された製品

Cisco IOS XR は該当しません。

Cisco 製品で稼働しているソフトウェアを確認するには、デバイスにログインし、**show version** コマンドを発行してシステム バナーを表示します。 Cisco IOS ソフトウェアは「Internetwork Operating System Software」または単に「IOS」と表示されます。 出力次の行で、イメージ名は「バージョンに」先行しているかっこと IOSリリース名の間で表示する。 その他の Cisco デバイスには **show version** コマンドがないか、異なる出力が返されます。

次の例は C3640-I-M のインストール済みイメージ名前と IOS リリース 12.3(6) を実行する Cisco製品を指定したものです:

```
Router>show ip http server status
HTTP server status: Disabled
```

次 の 例は C3845-ADVIPSERVICESK9-M のイメージ名と IOS リリース 12.3(11)T3 を実行する製品を示します:

```
Router>show ip http server status
HTTP server status: Disabled
```

Cisco IOS リリース指名についてのその他の情報は http://www.cisco.com/warp/public/620/1.html で見つけることができます。

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

Revision 2.0	29-March-2010	ソフトウェア バージョン および 修正 セクションをアップデートしました。
リビジョン 1.3	22-October-2009	不正利用事例と公式発表を追加研究者情報を含むためにアップデートしました。
リビジョン 1.2	19-June-2009	*ディセーブルを HTTP WEB_EXEC サービス* セクション修正しました。
リビジョン 1.1	14-January-2006	追加された追加諮問クレジット。
リビジ	1-	初回公開リリース

ョン 1.0	December-2005	

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。