

# ActiveState ActivePerl Path Revealing Vulnerability

分類 Other  
 関連ツール名称 なし  
 再現性 リモート

## 技術解説

### 1) 概要

ActivePerlを使用しているIISに対して、拡張子が .pl であり、かつサーバー上に存在しないファイルをリクエストすることで、本来参照できないはずのディレクトリの絶対パスが表示される。この脆弱性を利用することにより、リモートから攻撃に有用な情報が取得されてしまう可能性がある。

### 2) 原因

ActivePerlをインストールすると、拡張子が .pl であるファイルに対するリクエストを perl.exe が処理するようにIISのマッピングが自動的に追加される。

拡張子が .pl であり、かつサーバー上に存在しないファイルをリクエストすると、CGI Errorとしてリクエストされたファイル名とともにエラーメッセージを表示する。このとき表示されるファイル名は相対パスではなく絶対パスで記述されている。

# ActiveState ActivePerl Path Revealing Vulnerability

## 検証有無

結果 ○: 成功、×: 失敗、-: 未検証

サービス	アプリケーション	バージョン	結果
IIS 4.0	Active Perl	5.6.1	○
IIS 5.0			○
上記以外			-

## 検証結果

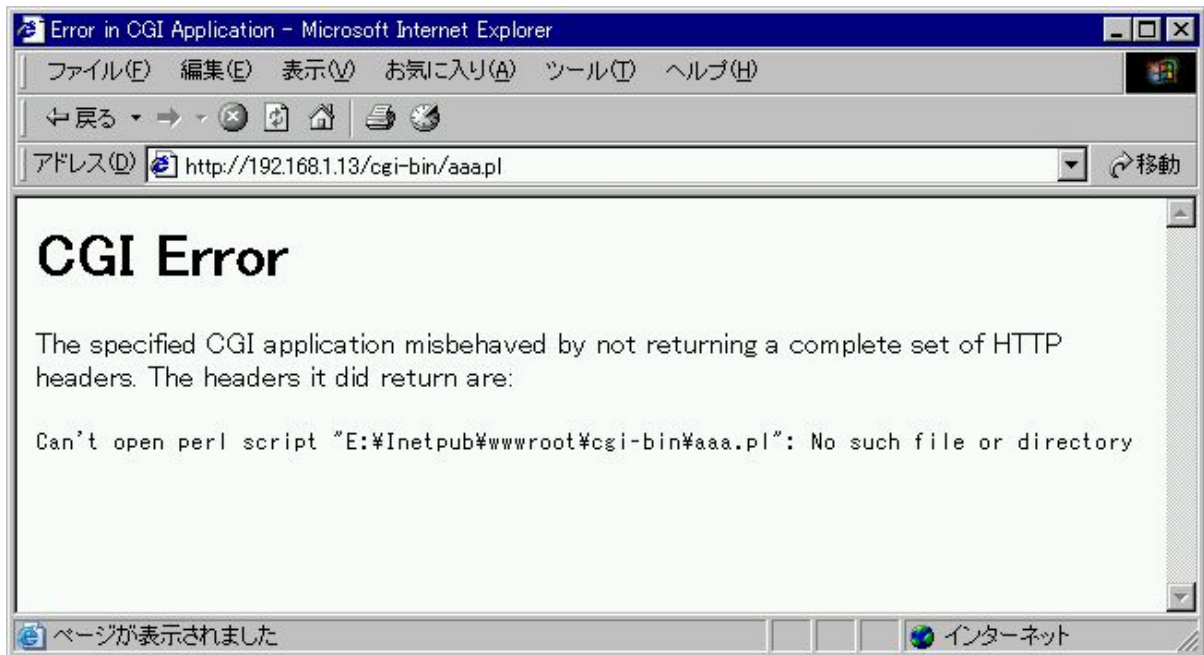
### 1) 検証環境

	OS	サービス	アプリケーション	備考
攻撃側	Windows NT 4.0 SP6a (J)			
ターゲット	Windows NT 4.0 SP6a (J)	IIS 4.0	Active Perl 5.6.1	
	Windows 2000 Advanced Server SP2 (J)	IIS 5.0		

## 2) 検証結果

<Windows NT 4.0 SP6a + IIS 4.0>

下図のように、絶対パスが表示されているのを確認した。



<Windows 2000 SP2 + IIS 5.0>

IIS 4.0 の場合と同様、絶対パスが表示されているのを確認した。

## 痕跡

### 1) ログ

<Windows NT 4.0 SP6a + IIS 4.0>

IISのアクセスログに以下のログが記録された。

```
01:13:26 192.168.1.13 GET /_vti_bin/aaa.pl 502
```

イベントログにはなにも出力されなかった。

<Windows 2000 SP2 + IIS 5.0>

Windows NT 4.0 SP6a + IIS 4.0 の場合と同様のログが記録された。

### 2) 痕跡

なし

## 影響

本来参照できないはずのディレクトリの絶対パスがリモートから参照されてしまい、攻

撃者に有用な情報を与えてしまう可能性がある。

なお、IISの[アプリケーション拡張子マッピングの追加/編集]で、[ファイルの存在を確認する]が有効になっている場合は、この問題の影響を受けない。

## 影響を受けるOS、サービス

影響 ○:脆弱性あり、×:脆弱性なし

(2002/1/2現在)

サービス	アプリケーション	バージョン	影響	備考
IIS	ActivePerl	5.6.1	○	「ファイルの存在を確認する」設定が無効になっているときのみ

OS、サービス Microsoft IIS 4.0  
Microsoft IIS 5.0  
アプリケーション ActivePerl 5.6.1

## 対策方法

### 1)対策

2002年1月22日現在、パッチは公開されていない。

[アプリケーション拡張子マッピングの追加/編集]で、[ファイルの存在を確認する]という設定を有効にすることで問題を回避可能である。

### 2) Advisory情報

---

Copyright © 2002 警察庁