# CWE Detail – CWE-67

## Description

The product constructs pathnames from user input, but it does not handle or incorrectly handles a pathname containing a Windows device name such as AUX or CON. This typically leads to denial of service or an information exposure when the application attempts to process the pathname as a regular file.

## Extended Description

Not properly handling virtual filenames (e.g. AUX, CON, PRN, COM1, LPT1) can result in different types of vulnerabilities. In some cases an attacker can request a device via injection of a virtual filename in a URL, which may cause an error that leads to a denial of service or an error page that reveals sensitive information. A product that allows device names to bypass filtering runs the risk of an attacker injecting malicious code in a file with the name of a device.

## Threat-Mapped Scoring

Score: 3.1

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2002-0106: Server allows remote attackers to cause a denial of service via a series of requests to .JSP files that contain an MS-DOS device name.

**•** CVE-2002-0200: Server allows remote attackers to cause a denial of service via an HTTP request for an MS-DOS device name.

**•** CVE-2002-1052: Product allows remote attackers to use MS-DOS device names in HTTP requests to cause a denial of service or obtain the physical path of the server.

**•** CVE-2001-0493: Server allows remote attackers to cause a denial of service via a URL that contains an MS-DOS device name.

**•** CVE-2001-0558: Server allows a remote attacker to create a denial of service via a URL request which includes a MS-DOS device name.

**•** CVE-2000-0168: Microsoft Windows 9x operating systems allow an attacker to cause a denial of service via a pathname that includes file device names, aka the "DOS Device in Path Name" vulnerability.

**•** CVE-2001-0492: Server allows remote attackers to determine the physical path of the server via a URL containing MS-DOS device names.

**•** CVE-2004-0552: Product does not properly handle files whose names contain reserved MS-DOS device names, which can allow malicious code to bypass detection when it is installed, copied, or executed.

**•** CVE-2005-2195: Server allows remote attackers to cause a denial of service (application crash) via a URL with a filename containing a .cgi extension and an MS-DOS device name.

## Modes of Introduction

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: DoS: Crash, Exit, or Restart, Read Application Data, Other — Notes:

## Potential Mitigations

**•** Implementation: Be familiar with the device names in the operating system where your system is deployed. Check input for these device names. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)