# CWE Detail – CWE-622

## Description

The product adds hooks to user-accessible API functions, but it does not properly validate the arguments. This could lead to resultant vulnerabilities.

## Extended Description

Such hooks can be used in defensive software that runs with privileges, such as anti-virus or firewall, which hooks kernel calls. When the arguments are not validated, they could be used to bypass the protection scheme or attack the product itself.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2007-0708: DoS in firewall using standard Microsoft functions

**•** CVE-2006-7160: DoS in firewall using standard Microsoft functions

**•** CVE-2007-1376: function does not verify that its argument is the proper type, leading to arbitrary memory write

**•** CVE-2007-1220: invalid syscall arguments bypass code execution limits

**•** CVE-2006-4541: DoS in IDS via NULL argument

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Unexpected State — Notes:

## Potential Mitigations

**•** Architecture and Design: Ensure that all arguments are verified, as defined by the API you are protecting. (Effectiveness: N/A)

**•** Architecture and Design: Drop privileges before invoking such functions, if possible. (Effectiveness: N/A)

## Applicable Platforms

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