# CWE Detail – CWE-1177

## Description

The product uses a function, library, or third party component
 that has been explicitly prohibited, whether by the developer or
 the customer.

## Extended Description

The developer - or customers - may wish to restrict or eliminate use of a function, library, or third party component for any number of reasons, including real or suspected vulnerabilities; difficulty to use securely; export controls or license requirements; obsolete or poorly-maintained code; internal code being scheduled for deprecation; etc. To reduce risk of vulnerabilities, the developer might maintain a list of "banned" functions that programmers must avoid using because the functions are difficult or impossible to use securely. This issue can also make the product more costly and difficult to maintain.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2007-1470: Library has multiple buffer overflows using sprintf() and strcpy()

**•** CVE-2007-4004: FTP client uses inherently insecure gets() function and is setuid root on some systems, allowing buffer overflow

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Reduce Maintainability — Notes:

## Demonstrative Examples

**•** However, gets() is inherently unsafe, because it copies all input from STDIN to the buffer without checking size. This allows the user to provide a string that is larger than the buffer size, resulting in an overflow condition.

**•** However, the programmer does not ensure that the size of the data pointed to by string will fit in the local buffer and copies the data with the potentially dangerous strcpy() function. This may result in a buffer overflow condition if an attacker can influence the contents of the string parameter.