# CWE Detail – CWE-234

## Description

If too few arguments are sent to a function, the function will still pop the expected number of arguments from the stack. Potentially, a variable number of arguments could be exhausted in a function as well.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2004-0276: Server earlier allows remote attackers to cause a denial of service (crash) via an HTTP request with a sequence of "%" characters and a missing Host field.

**•** CVE-2002-1488: Chat client allows remote malicious IRC servers to cause a denial of service (crash) via a PART message with (1) a missing channel or (2) a channel that the user is not in.

**•** CVE-2002-1169: Proxy allows remote attackers to cause a denial of service (crash) via an HTTP request to helpout.exe with a missing HTTP version numbers.

**•** CVE-2000-0521: Web server allows disclosure of CGI source code via an HTTP request without the version number.

**•** CVE-2001-0590: Application server allows a remote attacker to read the source code to arbitrary 'jsp' files via a malformed URL request which does not end with an HTTP protocol specification.

**•** CVE-2003-0239: Chat software allows remote attackers to cause a denial of service via malformed GIF89a headers that do not contain a GCT (Global Color Table) or an LCT (Local Color Table) after an Image Descriptor.

**•** CVE-2002-1023: Server allows remote attackers to cause a denial of service (crash) via an HTTP GET request without a URI.

**•** CVE-2002-1236: CGI crashes when called without any arguments.

**•** CVE-2003-0422: CGI crashes when called without any arguments.

**•** CVE-2002-1531: Crash in HTTP request without a Content-Length field.

**•** CVE-2002-1077: Crash in HTTP request without a Content-Length field.

**•** CVE-2002-1358: Empty elements/strings in protocol test suite affect many SSH2 servers/clients.

**•** CVE-2003-0477: FTP server crashes in PORT command without an argument.

**•** CVE-2002-0107: Resultant infoleak in web server via GET requests without HTTP/1.0 version string.

**•** CVE-2002-0596: GET request with empty parameter leads to error message infoleak (path disclosure).

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Execute Unauthorized Code or Commands, Gain Privileges or Assume Identity — Notes: There is the potential for arbitrary code execution with privileges of the vulnerable program if function parameter list is exhausted.

**•** Impact: DoS: Crash, Exit, or Restart — Notes: Potentially a program could fail if it needs more arguments then are available.

## Potential Mitigations

**•** Build and Compilation: This issue can be simply combated with the use of proper build process. (Effectiveness: N/A)

**•** Implementation: Forward declare all functions. This is the recommended solution. Properly forward declaration of all used functions will result in a compiler error if too few arguments are sent to a function. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** This can be exploited to disclose information with no work whatsoever. In fact, each time this function is run, it will print out the next 4 bytes on the stack after the two numbers sent to it.

## Notes

**•** Maintenance: This entry will be deprecated in a future version of CWE. The term "missing parameter" was used in both PLOVER and CLASP, with completely different meanings. However, data from both taxonomies was merged into this entry. In PLOVER, it was meant to cover malformed inputs that do not contain required parameters, such as a missing parameter in a CGI request. This entry's observed examples and classification came from PLOVER. However, the description, demonstrative example, and other information are derived from CLASP. They are related to an incorrect number of function arguments, which is already covered by CWE-685.