# CWE Detail – CWE-130

## Description

The product parses a formatted message or structure, but it does not handle or incorrectly handles a length field that is inconsistent with the actual length of the associated data.

## Extended Description

If an attacker can manipulate the length parameter associated with an input such that it is inconsistent with the actual length of the input, this can be leveraged to cause the target application to behave in unexpected, and possibly, malicious ways. One of the possible motives for doing so is to pass in arbitrarily large input to the application. Another possible motivation is the modification of application state by including invalid data for subsequent properties of the application. Such weaknesses commonly lead to attacks such as buffer overflows and execution of arbitrary code.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2014-0160: Chain: "Heartbleed" bug receives an inconsistent length parameter (CWE-130) enabling an out-of-bounds read (CWE-126), returning memory that could include private cryptographic keys and other sensitive data. (KEV)

**•** CVE-2009-2299: Web application firewall consumes excessive memory when an HTTP request contains a large Content-Length value but no POST data.

**•** CVE-2001-0825: Buffer overflow in internal string handling routine allows remote attackers to execute arbitrary commands via a length argument of zero or less, which disables the length check.

**•** CVE-2001-1186: Web server allows remote attackers to cause a denial of service via an HTTP request with a content-length value that is larger than the size of the request, which prevents server from timing out the connection.

**•** CVE-2001-0191: Service does not properly check the specified length of a cookie, which allows remote attackers to execute arbitrary commands via a buffer overflow, or brute force authentication by using a short cookie length.

**•** CVE-2003-0429: Traffic analyzer allows remote attackers to cause a denial of service and possibly execute arbitrary code via invalid IPv4 or IPv6 prefix lengths, possibly triggering a buffer overflow.

**•** CVE-2000-0655: Chat client allows remote attackers to cause a denial of service or execute arbitrary commands via a JPEG image containing a comment with an illegal field length of 1.

**•** CVE-2004-0492: Server allows remote attackers to cause a denial of service and possibly execute arbitrary code via a negative Content-Length HTTP header field causing a heap-based buffer overflow.

**•** CVE-2004-0201: Help program allows remote attackers to execute arbitrary commands via a heap-based buffer overflow caused by a .CHM file with a large length field

**•** CVE-2003-0825: Name services does not properly validate the length of certain packets, which allows attackers to cause a denial of service and possibly execute arbitrary code. Can overlap zero-length issues

**•** CVE-2004-0095: Policy manager allows remote attackers to cause a denial of service (memory consumption and crash) and possibly execute arbitrary code via an HTTP POST request with an invalid Content-Length value.

**•** CVE-2004-0826: Heap-based buffer overflow in library allows remote attackers to execute arbitrary code via a modified record length field in an SSLv2 client hello message.

**•** CVE-2004-0808: When domain logons are enabled, server allows remote attackers to cause a denial of service via a SAM\_UAS\_CHANGE request with a length value that is larger than the number of structures that are provided.

**•** CVE-2002-1357: Multiple SSH2 servers and clients do not properly handle packets or data elements with incorrect length specifiers, which may allow remote attackers to cause a denial of service or possibly execute arbitrary code.

**•** CVE-2004-0774: Server allows remote attackers to cause a denial of service (CPU and memory exhaustion) via a POST request with a Content-Length header set to -1.

**•** CVE-2004-0989: Multiple buffer overflows in xml library that may allow remote attackers to execute arbitrary code via long URLs.

**•** CVE-2004-0568: Application does not properly validate the length of a value that is saved in a session file, which allows remote attackers to execute arbitrary code via a malicious session file (.ht), web site, or Telnet URL contained in an e-mail message, triggering a buffer overflow.

**•** CVE-2003-0327: Server allows remote attackers to cause a denial of service via a remote password array with an invalid length, which triggers a heap-based buffer overflow.

**•** CVE-2003-0345: Product allows remote attackers to cause a denial of service and possibly execute arbitrary code via an SMB packet that specifies a smaller buffer length than is required.

**•** CVE-2004-0430: Server allows remote attackers to execute arbitrary code via a LoginExt packet for a Cleartext Password User Authentication Method (UAM) request with a PathName argument that includes an AFPName type string that is longer than the associated length field.

**•** CVE-2005-0064: PDF viewer allows remote attackers to execute arbitrary code via a PDF file with a large /Encrypt /Length keyLength value.

**•** CVE-2004-0413: SVN client trusts the length field of SVN protocol URL strings, which allows remote attackers to cause a denial of service and possibly execute arbitrary code via an integer overflow that leads to a heap-based buffer overflow.

**•** CVE-2004-0940: Is effectively an accidental double increment of a counter that prevents a length check conditional from exiting a loop.

**•** CVE-2002-1235: Length field of a request not verified.

**•** CVE-2005-3184: Buffer overflow by modifying a length value.

## Related Attack Patterns (CAPEC)

* CAPEC-47

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Memory, Modify Memory, Varies by Context — Notes:

## Potential Mitigations

**•** Implementation: When processing structured incoming data containing a size field followed by raw data, ensure that you identify and resolve any inconsistencies between the size field and the actual size of the data. (Effectiveness: N/A)

**•** Implementation: Do not let the user control the size of the buffer. (Effectiveness: N/A)

**•** Implementation: Validate that the length of the user-supplied data is consistent with the buffer size. (Effectiveness: N/A)

## Applicable Platforms

**•** C (Class: None, Prevalence: Sometimes)

**•** C++ (Class: None, Prevalence: Sometimes)

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

## Demonstrative Examples

**•** However, the message length variable from the structure is used as the condition for ending the for loop without validating that the message length variable accurately reflects the length of the message body (CWE-606). This can result in a buffer over-read (CWE-125) by reading from memory beyond the bounds of the buffer if the message length variable indicates a length that is longer than the size of a message body (CWE-130).

## Notes

**•** Relationship: This probably overlaps other categories including zero-length issues.