# CWE Detail – CWE-680

## Description

The product performs a calculation to determine how much memory to allocate, but an integer overflow can occur that causes less memory to be allocated than expected, leading to a buffer overflow.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2021-43537: Chain: in a web browser, an unsigned 64-bit integer is forcibly cast to a 32-bit integer (CWE-681) and potentially leading to an integer overflow (CWE-190). If an integer overflow occurs, this can cause heap memory corruption (CWE-122)

**•** CVE-2017-1000121: chain: unchecked message size metadata allows integer overflow (CWE-190) leading to buffer overflow (CWE-119).

## Related Attack Patterns (CAPEC)

* CAPEC-10
* CAPEC-100
* CAPEC-14
* CAPEC-24
* CAPEC-45
* CAPEC-46
* CAPEC-47
* CAPEC-67
* CAPEC-8
* CAPEC-9
* CAPEC-92

## Common Consequences

**•** Impact: Modify Memory, DoS: Crash, Exit, or Restart, Execute Unauthorized Code or Commands — Notes:

## Applicable Platforms

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

## Demonstrative Examples

**•** This code intends to allocate a table of size num\_imgs, however as num\_imgs grows large, the calculation determining the size of the list will eventually overflow (CWE-190). This will result in a very small list to be allocated instead. If the subsequent code operates on the list as if it were num\_imgs long, it may result in many types of out-of-bounds problems (CWE-119).