# CVE Detail – CVE-2022-0545

An integer overflow in the processing of loaded 2D images leads to a write-what-where vulnerability and an out-of-bounds read vulnerability, allowing an attacker to leak sensitive information or achieve code execution in the context of the Blender process when a specially crafted image file is loaded. This flaw affects Blender versions prior to 2.83.19, 2.93.8 and 3.1.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.48585

## CVSS Scoring

CVSS v3.1 Score: 7.8

Severity: HIGH

## Mapped CWE(s)

* CWE-190: Integer Overflow or Wraparound

## CAPEC(s)

* CAPEC-92: Forced Integer Overflow

## Affected Products

* cpe:2.3:a:blender:blender:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:blender:blender:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:blender:blender:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:10.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:11.0:\*:\*:\*:\*:\*:\*:\*