# CVE Detail – CVE-2019-1010006

Evince 3.26.0 is affected by buffer overflow. The impact is: DOS / Possible code execution. The component is: backend/tiff/tiff-document.c. The attack vector is: Victim must open a crafted PDF file. The issue occurs because of an incorrect integer overflow protection mechanism in tiff\_document\_render and tiff\_document\_get\_thumbnail.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.66648

## CVSS Scoring

CVSS v3.1 Score: 7.8

Severity: HIGH

## Mapped CWE(s)

* CWE-190: Integer Overflow or Wraparound
* CWE-787: Out-of-bounds Write

## CAPEC(s)

* CAPEC-92: Forced Integer Overflow

## Affected Products

* cpe:2.3:a:gnome:evince:3.26.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:16.04:\*:\*:\*:esm:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:8.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:9.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:10.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:leap:15.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:leap:15.1:\*:\*:\*:\*:\*:\*:\*