# CVE Detail – CVE-2018-10887

A flaw was found in libgit2 before version 0.27.3. It has been discovered that an unexpected sign extension in git\_delta\_apply function in delta.c file may lead to an integer overflow which in turn leads to an out of bound read, allowing to read before the base object. An attacker may use this flaw to leak memory addresses or cause a Denial of Service.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.71753

## CVSS Scoring

CVSS v3.1 Score: 8.1

Severity: HIGH

## Mapped CWE(s)

* CWE-125: Out-of-bounds Read
* CWE-190: Integer Overflow or Wraparound
* CWE-194: Unexpected Sign Extension
* CWE-681: Incorrect Conversion between Numeric Types

## CAPEC(s)

* CAPEC-540: Overread Buffers
* CAPEC-92: Forced Integer Overflow

## Affected Products

* cpe:2.3:a:libgit2:libgit2:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:8.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:9.0:\*:\*:\*:\*:\*:\*:\*