# CVE Detail – CVE-2019-13351

posix/JackSocket.cpp in libjack in JACK2 1.9.1 through 1.9.12 (as distributed with alsa-plugins 1.1.7 and later) has a "double file descriptor close" issue during a failed connection attempt when jackd2 is not running. Exploitation success depends on multithreaded timing of that double close, which can result in unintended information disclosure, crashes, or file corruption due to having the wrong file associated with the file descriptor.

## Threat-Mapped Scoring

Score: 2.3

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.49562

## CVSS Scoring

CVSS v3.0 Score: 8.1

Severity: HIGH

## Affected Products

* cpe:2.3:a:jackaudio:jack2:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:alsa-project:alsa:\*:\*:\*:\*:\*:\*:\*:\*