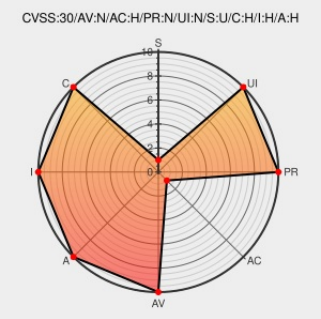
CVE-2019-13351

Published on: 07/05/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:45 PM UTC

CVE-2019-13351

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Alsa from Alsa-project contain the following vulnerability:

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.

CVE-2019-13351 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Set fSocket to -1 after close on an error to prevent a double close, by yaaii	Patch	MISC

Set fSocket to -1 after close on an error to prevent a double close. by yasij · Pull Request #480 · jackaudio/jack2 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/jackaudio/jack2/pull/480
Sporadic crash when during on my TV/Receiver due to double close() on the same fd in ActiveAE · Issue #16258 · xbmc/xbmc · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/xbmc/xbmc/issues/16258

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Alsa-project	Alsa	All	All	All	All
Application	Jackaudio	Jack2	All	All	All	All

cpe:2.3:a:alsa-project:alsa:*:*:*:*:*:*:*:*:

cpe:2.3:a:jackaudio:jack2:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→