



CVE-2019-19727

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2019-19727
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-13 19:15:00 UTC
Updated	2020-01-23 13:38:00 UTC
Description	SchedMD Slurm before 18.08.9 and 19.x before 19.05.5 has weak slurmdbd.conf permissions.

Risk And Classification

Problem Types: CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Schedmd	Slurm	All	All	All	All
Application	Schedmd	Slurm	All	All	All	All

References

Reference	Source	Link
The slurm-announce Archives	MISC	lists.schedmd
News SchedMD	CONFIRM	www.schedmd
[security-announce] openSUSE-SU-2020:0085-1: important: Security update	SUSE	lists.opensuse
Bug 1155784 – VUL-0: CVE-2019-19727: slurm: slurmdbd: slurmdbd.conf has an insecure Permission by default	MISC	bugzilla.suse
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)