



CVE-2022-45132

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-45132
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-18 23:15:00 UTC
Updated	2023-11-07 03:54:00 UTC
Description	In Linaro Automated Validation Architecture (LAVA) before 2022.11.1, remote code execution can be achieved through use

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linaro	Lava	All	All	All	All

References

Reference	Source	Link	Tags
Python vulnerabilities : Code execution in jinja templates - Podalirius	MISC	podalirius.net	
Two security vulnerabilities in LAVA server - Lava-announce - op-lists.linaro.org		lists.lavasoftware.org	
Two security vulnerabilities in LAVA server - Lava-announce - op-lists.linaro.org	MISC	lists.lavasoftware.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

183840 Debian Security Update for lava (CVE-2022-45132)

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