



CVE-2023-38496

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

Summary

CVE	CVE-2023-38496
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-25 22:15:00 UTC
Updated	2023-08-02 19:32:00 UTC
Description	Apptainer is an open source container platform. Version 1.2.0-rc.2 introduced an ineffective privilege drop when requesting

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lfprojects	Apptainer	1.2.0	-	All	All
Application	Lfprojects	Apptainer	1.2.0	rc2	All	All

References

Reference

- Set real UID to zero when escalating privileges for CNI plugins to fix issue appeared with RHEL 9.X (release 1.2) by cclerget · Pull Request #1
- Restore old syscall setresuid behavior when escalating/dropping privileges. by cclerget · Pull Request #1578 · apptainer/apptainer · GitHub
- Ineffective privileges drop when requesting container network · Advisory · apptainer/apptainer · GitHub
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)