



CVE-2023-28642

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-28642
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-29 19:15:00 UTC
Updated	2023-11-07 04:10:00 UTC
Description	runc is a CLI tool for spawning and running containers according to the OCI specification. It was found that AppArmor can b

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Runc	All	All	All	All

References

Reference	Source	Link
AppArmor/SELinux bypass with symlinked /proc · Advisory · opencontainers/runc · GitHub	MISC	github.c
[1.1 backport] Prohibit /proc and /sys to be symlinks by thaJeztah · Pull Request #3785 · opencontainers/runc · GitHub	MISC	github.c
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160789 Oracle Enterprise Linux Security Update for aardvark-dns (ELSA-2023-12579)

160797 Oracle Enterprise Linux Security Update for buildah (ELSA-2023-12578)

161114 Oracle Enterprise Linux Security Update for runc (ELSA-2023-6380)

161175 Oracle Enterprise Linux Security Update for container-tools:ol8 (ELSA-2023-6939)

161187 Oracle Enterprise Linux Security Update for container-tools:4.0 (ELSA-2023-6938)
182389 Debian Security Update for runc (CVE-2023-28642)
199349 Ubuntu Security Notification for runC Vulnerabilities (USN-6088-1)
199528 Ubuntu Security Notification for runC Vulnerabilities (USN-6088-2)
242301 Red Hat Update for runc (RHSA-2023:6380)
242415 Red Hat Update for container-tools:rhel8 (RHSA-2023:6939)
242458 Red Hat Update for container-tools:4.0 (RHSA-2023:6938)
242773 Red Hat Update for container-tools:3.0 (RHSA-2024:0564)
355356 Amazon Linux Security Advisory for runc : ALAS2NITRO-ENCLAVES-2023-024
355359 Amazon Linux Security Advisory for runc : ALAS2DOCKER-2023-025
355440 Amazon Linux Security Advisory for runc : ALAS2023-2023-208
355564 Amazon Linux Security Advisory for runc : ALAS2ECS-2023-004
379641 Alibaba Cloud Linux Security Update for container-tools:rhel8 (ALINUX3-SA-2024:0050)
502953 Alpine Linux Security Update for runc
503262 Alpine Linux Security Update for runc
506236 Alpine Linux Security Update for runc
6140060 AWS Bottlerocket Security Update for runc (GHSA-h3xm-qgch-xvpp)
673273 EulerOS Security Update for docker-runc (EulerOS-SA-2023-2581)
673302 EulerOS Security Update for docker-runc (EulerOS-SA-2023-2611)
673898 EulerOS Security Update for docker-runc (EulerOS-SA-2023-2680)
673972 EulerOS Security Update for docker-runc (EulerOS-SA-2023-2638)
753943 SUSE Enterprise Linux Security Update for runc (SUSE-SU-2023:2003-1)
906794 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-runc (25886-1)
906875 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-runc (25850-1)
941400 AlmaLinux Security Update for runc (ALSA-2023:6380)
941444 AlmaLinux Security Update for container-tools:4.0 (ALSA-2023:6938)
941481 AlmaLinux Security Update for container-tools:rhel8 (ALSA-2023:6939)

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](#).

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