



CVE-2021-41092

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

Summary

CVE	CVE-2021-41092
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-04 20:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	Docker CLI is the command line interface for the docker container runtime. A bug was found in the Docker CLI where running

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Docker	Command Line Interface	All	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All

References

Reference	Source	Link
Docker CLI leaks private registry credentials to registry-1.docker.io · Advisory · docker/cli · GitHub	CONFIRM	github.com
[SECURITY] Fedora 34 Update: moby-engine-20.10.9-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 34 Update: moby-engine-20.10.9-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
cert-portal.siemens.com/productcert/pdf/ssa-222547.pdf	CONFIRM	cert-portal.siemens.com
[SECURITY] Fedora 35 Update: moby-engine-20.10.9-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 35 Update: moby-engine-20.10.9-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Merge pull request #2 from moby/cli-ghsa-99pg-grm5-qq3v-default-authc... · docker/cli@893e52c · GitHub	MISC	github.com
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

179499	Debian Security Update for docker.io (CVE-2021-41092)
198560	Ubuntu Security Notification for Docker Vulnerability (USN-5134-1)
281996	Fedora Security Update for containerd (FEDORA-2021-df975338d4)
352849	Amazon Linux Security Advisory for docker: ALAS-2021-1537
353186	Amazon Linux Security Advisory for docker : ALAS2NITRO-ENCLAVES-2022-017
353191	Amazon Linux Security Advisory for docker : ALAS2DOCKER-2022-017
356876	Amazon Linux Security Advisory for docker : ALAS2ECS-2023-028
501837	Alpine Linux Security Update for docker
504679	Alpine Linux Security Update for docker
590976	Siemens SCALANCE LPE9403 Third-Party Multiple Vulnerabilities (ICSA-22-167-09) (SSA-222547)
6140407	AWS Bottlerocket Security Update for docker-cli (GHSA-vp43-f3pm-7jvp)
672019	EulerOS Security Update for docker-engine (EulerOS-SA-2022-2253)
672023	EulerOS Security Update for docker (EulerOS-SA-2022-2265)
672049	EulerOS Security Update for docker-engine (EulerOS-SA-2022-2240)
672074	EulerOS Security Update for docker-engine (EulerOS-SA-2022-2218)
672110	EulerOS Security Update for docker-engine (EulerOS-SA-2022-2311)
751272	SUSE Enterprise Linux Security Update for containerd, docker, runc (SUSE-SU-2021:3506-1)
751273	OpenSUSE Security Update for containerd, docker, runc (openSUSE-SU-2021:3506-1)
751303	OpenSUSE Security Update for containerd, docker, runc (openSUSE-SU-2021:1404-1)
751692	OpenSUSE Security Update for containerd, docker (openSUSE-SU-2022:0334-1)
753284	SUSE Enterprise Linux Security Update for containerd, docker (SUSE-SU-2022:0334-1)

© [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](#).

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