



CVE-2021-21284

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

Summary

CVE	CVE-2021-21284
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-02 18:15:00 UTC
Updated	2022-04-29 19:22:00 UTC
Description	In Docker before versions 9.03.15, 20.10.3 there is a vulnerability involving the --userns-remap option in which access to re

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Docker	Docker	All	All	All	All
Application	Docker	Docker	All	All	All	All
Application	Netapp	E-series Santricity Os Controller	All	All	All	All

References

Reference	Source	Link
Release v20.10.3 · moby/moby · GitHub	MISC	github.com
Merge pull request #41964 from thaJeztah/CVE-2021-21284_master · moby/moby@64bd448 · GitHub	MISC	github.com
Docker Engine release notes Docker Documentation	MISC	docs.docker.com
February 2021 Docker Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Release v19.03.15 · moby/moby · GitHub	MISC	github.com
Access to remapped root allows privilege escalation to real root · Advisory · moby/moby · GitHub	CONFIRM	github.com
Debian -- Security Information -- DSA-4865-1 docker.io	DEBIAN	www.debian.org
Docker: Multiple vulnerabilities (GLSA 202107-23) — Gentoo security	GENTOO	security.gentoo.org
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

174971 SUSE Enterprise Linux Security Update for containerd, docker, runc (SUSE-SU-2021:1458-1)
179597 Debian Security Update for docker.io (CVE-2021-21284)
352873 Amazon Linux Security Advisory for docker : ALAS-2021-1550
353057 Amazon Linux Security Advisory for docker : ALAS2NITRO-ENCLAVES-2021-001
353070 Amazon Linux Security Advisory for docker : ALAS2DOCKER-2021-001
356561 Amazon Linux Security Advisory for docker : ALAS2ECS-2023-015
500869 Alpine Linux Security Update for docker
504678 Alpine Linux Security Update for docker
6140344 AWS Bottlerocket Security Update for docker (GHSA-9hr9-47xc-fjgg)
671467 EulerOS Security Update for docker-engine (EulerOS-SA-2022-1424)
671480 EulerOS Security Update for docker-engine (EulerOS-SA-2022-1445)
671627 EulerOS Security Update for docker-engine (EulerOS-SA-2022-1644)
671641 EulerOS Security Update for docker-engine (EulerOS-SA-2022-1658)
710053 Gentoo Linux Docker Multiple vulnerabilities (GLSA 202107-23)
750155 SUSE Enterprise Linux Security Update for containerd, docker, runc (SUSE-SU-2021:1954-1)
750363 OpenSUSE Security Update for containerd, docker, docker-runc, golang-github-docker-libnetwork (openSUSE-SU-2021:0278-1)
750648 OpenSUSE Security Update for containerd, docker, runc (openSUSE-SU-2021:0878-1)
750812 OpenSUSE Security Update for containerd, docker, runc (openSUSE-SU-2021:1954-1)
900005 CBL-Mariner Linux Security Update for moby-buildx 0.4.1
900183 CBL-Mariner Linux Security Update for moby-engine 19.03.15
900184 CBL-Mariner Linux Security Update for moby-cli 19.03.15
903410 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-buildx (4426)
903630 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-engine (4568)
903637 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-cli (4428)

© [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](#)