



# CVE-2021-21285

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

## Summary

<b>CVE</b>	CVE-2021-21285
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-02-02 18:15:00 UTC
<b>Updated</b>	2022-10-25 12:55:00 UTC
<b>Description</b>	In Docker before versions 9.03.15, 20.10.3 there is a vulnerability in which pulling an intentionally malformed Docker image

## Risk And Classification

**Problem Types:** CWE-754

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Application	<a href="#">Docker</a>	<a href="#">Docker</a>	All	All	All	All
Application	<a href="#">Docker</a>	<a href="#">Docker</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">E-series Santricity Os Controller</a>	All	All	All	All

## References

Reference	Source	Link
Release v20.10.3 · moby/moby · GitHub	MISC	<a href="#">github.com</a>
Merge pull request #41966 from thaJeztah/CVE-2021-21285_master · moby/moby@8d31795 · GitHub	MISC	<a href="#">github.com</a>
Docker daemon crash during image pull of malicious image · Advisory · moby/moby · GitHub	CONFIRM	<a href="#">github.com</a>
Docker Engine release notes   Docker Documentation	MISC	<a href="#">docs.docker.com</a>
February 2021 Docker Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>
Release v19.03.15 · moby/moby · GitHub	MISC	<a href="#">github.com</a>
Debian -- Security Information -- DSA-4865-1 docker.io	DEBIAN	<a href="#">www.debian.org</a>
Docker: Multiple vulnerabilities (GLSA 202107-23) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">174971</a> SUSE Enterprise Linux Security Update for containerd, docker, runc (SUSE-SU-2021:1458-1)
<a href="#">179659</a> Debian Security Update for docker.io (CVE-2021-21285)
<a href="#">352873</a> Amazon Linux Security Advisory for docker : ALAS-2021-1550
<a href="#">353057</a> Amazon Linux Security Advisory for docker : ALAS2NITRO-ENCLAVES-2021-001
<a href="#">353070</a> Amazon Linux Security Advisory for docker : ALAS2DOCKER-2021-001
<a href="#">356561</a> Amazon Linux Security Advisory for docker : ALAS2ECS-2023-015
<a href="#">500869</a> Alpine Linux Security Update for docker
<a href="#">504678</a> Alpine Linux Security Update for docker
<a href="#">6140083</a> AWS Bottlerocket Security Update for docker (GHSA-cf37-ggjp-fg7r)
<a href="#">670328</a> EulerOS Security Update for docker-engine (EulerOS-SA-2021-1896)
<a href="#">670355</a> EulerOS Security Update for docker-engine (EulerOS-SA-2021-1869)
<a href="#">670382</a> EulerOS Security Update for docker-engine (EulerOS-SA-2021-1943)
<a href="#">670403</a> EulerOS Security Update for docker-engine (EulerOS-SA-2021-1922)
<a href="#">710053</a> Gentoo Linux Docker Multiple vulnerabilities (GLSA 202107-23)
<a href="#">750155</a> SUSE Enterprise Linux Security Update for containerd, docker, runc (SUSE-SU-2021:1954-1)
<a href="#">750363</a> OpenSUSE Security Update for containerd, docker, docker-runc, golang-github-docker-libnetwork (openSUSE-SU-2021:0278-1)
<a href="#">750648</a> OpenSUSE Security Update for containerd, docker, runc (openSUSE-SU-2021:0878-1)
<a href="#">750812</a> OpenSUSE Security Update for containerd, docker, runc (openSUSE-SU-2021:1954-1)
<a href="#">900005</a> CBL-Mariner Linux Security Update for moby-buildx 0.4.1
<a href="#">900183</a> CBL-Mariner Linux Security Update for moby-engine 19.03.15
<a href="#">900184</a> CBL-Mariner Linux Security Update for moby-cli 19.03.15
<a href="#">903228</a> Common Base Linux Mariner (CBL-Mariner) Security Update for moby-engine (4569)
<a href="#">903264</a> Common Base Linux Mariner (CBL-Mariner) Security Update for moby-cli (4429)
<a href="#">903303</a> Common Base Linux Mariner (CBL-Mariner) Security Update for moby-buildx (4427)

© [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](#)**