CVE-2021-21285

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-21285
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	2022-10-25 12:55:00 UTC
Description	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	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 #41966 from thaJeztah/CVE-2021-21285_master · moby/moby@8d31795 · GitHub	MISC	github.com
Docker daemon crash during image pull of malicious image · Advisory · moby/moby · GitHub	CONFIRM	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
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

NVD vulnerability detail NVD nvd.nist.gov

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)

179659 Debian Security Update for docker.io (CVE-2021-21285)

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

6140083 AWS Bottlerocket Security Update for docker (GHSA-cf37-ggjp-fg7r)

670328 EulerOS Security Update for docker-engine (EulerOS-SA-2021-1896)

670355 EulerOS Security Update for docker-engine (EulerOS-SA-2021-1869)

670382 EulerOS Security Update for docker-engine (EulerOS-SA-2021-1943)

670403 EulerOS Security Update for docker-engine (EulerOS-SA-2021-1922)

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

903228 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-engine (4569)

903264 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-cli (4429)

903303 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-buildx (4427)

997027 GO (Go) Security Update for github.com/moby/moby (GHSA-6fj5-m822-rqx8)