



CVE-2020-15257

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

Summary

CVE	CVE-2020-15257
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-01 03:15:00 UTC
Updated	2023-11-07 03:17:00 UTC
Description	containerd is an industry-standard container runtime and is available as a daemon for Linux and Windows. In containerd be

Risk And Classification

Problem Types: CWE-669

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	Fedoraproject	Fedora	33	All	All	All
Application	Linuxfoundation	Containerd	All	All	All	All
Application	Linuxfoundation	Containerd	All	All	All	All

References

Reference	Source	Link
containerd-shim API Exposed to Host Network Containers · Advisory · containerd/containerd · GitHub	CONFIRM	github.com
Merge pull request from GHSA-36xw-fx78-c5r4 · containerd/containerd@4a4bb85 · GitHub	MISC	github.com
[SECURITY] Fedora 33 Update: containerd-1.4.3-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Release containerd 1.4.3 · containerd/containerd · GitHub	MISC	github.com
Debian -- Security Information -- DSA-4865-1 docker.io	DEBIAN	www.debian.org
[SECURITY] Fedora 33 Update: containerd-1.4.3-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
containerd: Multiple vulnerabilities (GLSA 202105-33) — 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

353047	Amazon Linux Security Advisory for containerd : ALAS2NITRO-ENCLAVES-2021-012
353060	Amazon Linux Security Advisory for containerd : ALAS2DOCKER-2021-012
356880	Amazon Linux Security Advisory for containerd : ALAS2ECS-2023-030
500858	Alpine Linux Security Update for containerd
500868	Alpine Linux Security Update for docker
501594	Alpine Linux Security Update for k3s
504640	Alpine Linux Security Update for containerd
504672	Alpine Linux Security Update for docker
6140365	AWS Bottlerocket Security Update for containerd (GHSA-9cqr-6mvg-w8jv)
671845	EulerOS Security Update for docker-engine (EulerOS-SA-2022-1886)
710081	Gentoo Linux containerd Multiple vulnerabilities (GLSA 202105-33)
750363	OpenSUSE Security Update for containerd, docker, docker-runc, golang-github-docker-libnetwork (openSUSE-SU-2021:0278-1)
982383	Go (go) Security Update for github.com/containerd/containerd/cmd (GHSA-36xw-fx78-c5r4)

© [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](#)