



# CVE-2021-43784

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

## Summary

<b>CVE</b>	CVE-2021-43784
<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>	2021-12-06 18:15:00 UTC
<b>Updated</b>	2021-12-08 18:05:00 UTC
<b>Description</b>	runc is a CLI tool for spawning and running containers on Linux according to the OCI specification. In runc, netlink is used in

## Risk And Classification

**Problem Types:** CWE-190

## 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>	9.0	All	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	All	All	All	All

## References

### Reference

- [SECURITY] [DLA 2841-1] runc security update
- Open bind mount sources from the host users · [opencontainers/runc@9c44407](#) · GitHub
- Merge pull request from GHSA-v95c-p5hm-xq8f · [opencontainers/runc@f50369a](#) · GitHub
- 2241 - project-zero - Project Zero - Monorail
- runc init: avoid netlink message length overflows · [opencontainers/runc@d72d057](#) · GitHub
- Overflow in netlink bytemsg length field allows attacker to override netlink-based container configuration · Advisory · [opencontainers/runc](#) · Git
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

161114 Oracle Enterprise Linux Security Update for runc (ELSA-2023-6380)
178929 Debian Security Update for runc (DLA 2841-1)
183127 Debian Security Update for runc (CVE-2021-43784)
199528 Ubuntu Security Notification for runC Vulnerabilities (USN-6088-2)
242301 Red Hat Update for runc (RHSA-2023:6380)
502183 Alpine Linux Security Update for runc
6000482 Debian Security Update for runc (DLA 3735-1)
6140096 AWS Bottlerocket Security Update for runc (GHSA-86p7-cxqj-3p24)
751555 OpenSUSE Security Update for runc (openSUSE-SU-2021:4171-1)
751558 OpenSUSE Security Update for runc (openSUSE-SU-2021:1625-1)
900460 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-runc (6295)
901615 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-runc (6682-1)
941400 AlmaLinux Security Update for runc (ALSA-2023:6380)

© [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](#)**