



# CVE-2019-16884

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-16884
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-09-25 18:15:00 UTC
<b>Updated</b>	2023-11-07 03:06:00 UTC
<b>Description</b>	runc through 1.0.0-rc8, as used in Docker through 19.03.2-ce and other products, allows AppArmor restriction bypass beca

## Risk And Classification

**Problem Types:** CWE-863

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.10	All	All	All
Application	<a href="#">Docker</a>	<a href="#">Docker</a>	All	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc1	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc2	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc3	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc4	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc5	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc6	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc7	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc8	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	All	All	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc1	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc2	All	All

Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc3	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc4	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc5	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc6	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc7	All	All
Application	<a href="#">Linuxfoundation</a>	<a href="#">Runc</a>	1.0.0	rc8	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.4	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	4.1	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	4.2	All	All	All

## References

Reference	Source
AppArmor can be bypassed by a malicious image that specifies a volume at /proc · Issue #2128 · opencontainers/runc · GitHub	MISC
[SECURITY] Fedora 31 Update: runc-1.0.0-101.rc9.gitc1485a1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA
[SECURITY] Fedora 30 Update: runc-1.0.0-95.rc9.gitc1485a1.fc30 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 31 Update: runc-1.0.0-101.rc9.gitc1485a1.fc31 - package-announce - Fedora Mailing-Lists	
Red Hat Customer Portal	REDHAT
CVE-2019-16884 Docker Vulnerability in NetApp Products   NetApp Product Security	CONFIRM
[security-announce] openSUSE-SU-2019:2434-1: moderate: Security update f	SUSE
[SECURITY] [DLA 3369-1] runc security update	MLIST
[security-announce] openSUSE-SU-2020:0045-1: moderate: Security update f	SUSE
[SECURITY] Fedora 30 Update: runc-1.0.0-95.rc9.gitc1485a1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA
Red Hat Customer Portal	REDHAT
[SECURITY] Fedora 29 Update: runc-1.0.0-95.rc9.gitc1485a1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA
Red Hat Customer Portal	REDHAT
[SECURITY] Fedora 29 Update: runc-1.0.0-95.rc9.gitc1485a1.fc29 - package-announce - Fedora Mailing-Lists	
[SECURITY] [DLA 3369-1] runc security update	MLIST

[SECURITY] [DLA 3322-1] goiang-github-opencontainers-selinux security update	MLISI
runC: Multiple vulnerabilities (GLSA 202003-21) — Gentoo security	GENTOO
[security-announce] openSUSE-SU-2019:2418-1: moderate: Security update f	SUSE
USN-4297-1: runC vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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)
- [181581](#) Debian Security Update for goiang-github-opencontainers-selinux (DLA 3322-1)
- [181640](#) Debian Security Update for runc (DLA 3369-1)
- [353050](#) Amazon Linux Security Advisory for runc : ALAS2NITRO-ENCLAVES-2021-009
- [353063](#) Amazon Linux Security Advisory for runc : ALAS2DOCKER-2021-009
- [353110](#) Amazon Linux Security Advisory for runc : ALAS-2021-1556
- [377335](#) Alibaba Cloud Linux Security Update for container-tools:rhel8 (ALINUX3-SA-2022:0110)
- [500855](#) Alpine Linux Security Update for containerd
- [501239](#) Alpine Linux Security Update for runc
- [504637](#) Alpine Linux Security Update for containerd
- [770009](#) Red Hat OpenShift Container Platform 4.1.24 Security Update (RHSA-2019:3940)
- [770011](#) Red Hat OpenShift Container Platform 4.2 Security Update (RHSA-2019:4074)
- [900005](#) CBL-Mariner Linux Security Update for moby-buildx 0.4.1
- [903055](#) Common Base Linux Mariner (CBL-Mariner) Security Update for moby-buildx (4423)
- [940571](#) AlmaLinux Security Update for container-tools:rhel8 (ALSA-2019:4269)
- [960726](#) Rocky Linux Security Update for container-tools:rhel8 (RLSA-2019:4269)

© 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](https://status.cve.report)**