CVE-2019-5736

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-5736
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-11 19:29:00 UTC
Updated	2024-02-02 12:15:00 UTC
Description	runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc bina

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Mesos	All	All	All	All
Application	Apache	Mesos	All	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	D2iq	Dc/os	All	All	All	All
Operating System	D2iq	Dc/os	All	All	All	All
Application	D2iq	Kubernetes Engine	All	All	All	All
Application	Docker	Docker	All	All	All	All
Application	Docker	Docker	All	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All

Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Application	Google	Kubernetes Engine	-	All	All	All
Application	Google	Kubernetes Engine	-	All	All	All
Application	Hp	Onesphere	-	All	All	All
Application	Hp	Onesphere	-	All	All	All
Application	Linuxcontainers	Lxc	All	All	All	All
Application	Linuxcontainers	Lxc	All	All	All	All
Application	Linuxfoundation	Runc	1.0.0	rc1	All	All
Application	Linuxfoundation	Runc	1.0.0	rc2	All	All
Application	Linuxfoundation	Runc	1.0.0	rc3	All	All
Application	Linuxfoundation	Runc	1.0.0	rc4	All	All
Application	Linuxfoundation	Runc	1.0.0	rc5	All	All
Application	Linuxfoundation	Runc	1.0.0	rc6	All	All
Application	Linuxfoundation	Runc	All	All	All	All
Application	Linuxfoundation	Runc	1.0.0	rc1	All	All
Application	Linuxfoundation	Runc	1.0.0	rc2	All	All
Application	Linuxfoundation	Runc	1.0.0	rc3	All	All
Application	Linuxfoundation	Runc	1.0.0	rc4	All	All
Application	Linuxfoundation	Runc	1.0.0	rc5	All	All
Application	Linuxfoundation	Runc	1.0.0	rc6	All	All
Operating System	Mesosphere	Dc/os	All	All	All	All
Operating System	Mesosphere	Dc/os	All	All	All	All
Application	Mesosphere	Kubernetes Engine	All	All	All	All
Application	Mesosphere	Kubernetes Engine	All	All	All	All
Application	Microfocus	Service Management Automation	2018.02	All	All	All
Application	Microfocus	Service Management Automation	2018.05	All	All	All
Application	Microfocus	Service Management Automation	2018.08	All	All	All
Application	Microfocus	Service Management Automation	2018.11	All	All	All
Application	Microfocus	Service Management Automation	2018.02	All	All	All
Application	Microfocus	Service Management Automation	2018.05	All	All	All
Application	Microfocus	Service Management Automation	2018.08	All	All	All
Application	Microfocus	Service Management Automation	2018.11	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All

Application	Netapp	Solidfire	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Opensuse	Backports Sle	15.0	-	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Application	Opensuse	Backports Sle	15.0	-	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Application	Redhat	Container Development Kit	3.7	All	All	All
Application	Redhat	Container Development Kit	3.7	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Application	Redhat	Openshift	3.4	All	All	All
Application	Redhat	Openshift	3.5	All	All	All
Application	Redhat	Openshift	3.6	All	All	All
Application	Redhat	Openshift	3.7	All	All	All
Application	Redhat	Openshift	3.4	All	All	All
Application	Redhat	Openshift	3.5	All	All	All
Application	Redhat	Openshift	3.6	All	All	All
Application	Redhat	Openshift	3.7	All	All	All

References

Reference	Source	Link
[security-announce] openSUSE-SU-2019:1444-1: important: Security update	SUSE	lists
oss-security - Re: Re: runc: CVE-2024-21626: high severity container breakout attack		www
[SECURITY] Fedora 29 Update: python3-lxc-3.0.4-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists
Pony Mail!		lists
oss-security - Re: Membership application for linux-distros - VMware	MLIST	www
CVE-2019-5736 and runC vulnerability in AKS | Azure updates | Microsoft Azure	MISC	azu
Pony Mail!	MLIST	lists

Runtimes And the Curse of the Privileged Container | brauner's blog	MISC	brau
Pony Mail!	MLIST	lists
Pony Mail!	MLIST	lists
GitHub - q3k/cve-2019-5736-poc: Unweaponized Proof of Concept for CVE-2019-5736 (Docker escape)	MISC	gith
CVE-2019-5736 fix for Azure IoT Edge | Azure updates | Microsoft Azure	MISC	azu
Dragon Sector: CVE-2019-5736: Escape from Docker and Kubernetes containers to root on host	MISC	blog
Red Hat Customer Portal	REDHAT	acc
[security-announce] openSUSE-SU-2019:2021-1: important: Security update	SUSE	lists
Pony Mail!		lists
oss-security - CVE-2019-5736: runc container breakout (all versions)	MISC	www
Container Security Issue (CVE-2019-5736)	MISC	aws
Pony Mail!		lists
[security-announce] openSUSE-SU-2019:1275-1: important: Security update	SUSE	lists
Pony Mail!	MLIST	lists
Pony Mail!		lists
Runc and CVE-2019-5736 - Kubernetes	MISC	kub
[security-announce] openSUSE-SU-2019:1079-1: important: Security update	SUSE	lists
Pony Mail!	MLIST	lists
Document Display | HPE Support Center	CONFIRM	sup
[SECURITY] Fedora 30 Update: lxcfs-3.0.4-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists
[security-announce] openSUSE-SU-2019:1499-1: important: Security update	SUSE	lists
[security-announce] openSUSE-SU-2019:1227-1: important: Security update	SUSE	lists
USN-4048-1: Docker vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn
[security-announce] openSUSE-SU-2019:1481-1: important: Security update	SUSE	lists
[security-announce] openSUSE-SU-2019:2286-1: moderate: Security update f	SUSE	lists
Docker runc Command Execution Proof Of Concept ≈ Packet Storm	MISC	pac
oss-security - runc: CVE-2024-21626: high severity container breakout attack		www
[SECURITY] Fedora 29 Update: runc-1.0.0-92.dev.gitc1b8c57.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists
Bug 1121967 – VUL-0: CVE-2019-5736: docker-runc: container breakout vulnerability	MISC	bug
runc < 1.0-rc6 (Docker < 18.09.2) - Container Breakout (2)	EXPLOIT-DB	www
Red Hat Customer Portal	REDHAT	acc
CVE-2019-5736 Opencontainers-runc Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	sec
oss-security - Re: linux-distros membership application - Microsoft	MLIST	www
MySupport - Micro Focus Software Support	CONFIRM	soft
Container Privilege Escalation Vulnerability Affecting Cisco Products: February 2019	CISCO	tool

[security-announce] openSUSE-SU-2019:1506-1: important: Security update	SUSE	lists
nsenter: clone /proc/self/exe to avoid exposing host binary to container · opencontainers/runc@0a8e411 · GitHub	MISC	gith
Pony Mail!		lists
[security-announce] openSUSE-SU-2019:2245-1: moderate: Security update f	SUSE	lists
Mitigating CVE-2019-5736 Impacting RunC and Docker | Twistlock	MISC	www
[SECURITY] Fedora 30 Update: runc-1.0.0-92.dev.gitc1b8c57.fc30 - package-announce - Fedora Mailing-Lists		lists
oss-security - Re: linux-distros membership application - Microsoft	MLIST	www
runc < 1.0-rc6 (Docker < 18.09.2) - Container Breakout (1) - Linux local Exploit	EXPLOIT-DB	www
runc - Malicious container escape - CVE-2019-5736 - Red Hat Customer Portal	MISC	acce
[SECURITY] Fedora 30 Update: runc-1.0.0-92.dev.gitc1b8c57.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists
Pony Mail!		lists
Pony Mail!		lists
merge branch 'cve-2019-5736' · opencontainers/runc@6635b4f · GitHub	MISC	gith
GitHub - rancher/runc-cve: CVE patches for legacy runc packaged with Docker	MISC	gith
Red Hat Customer Portal	MISC	acce
Release 18.09.2 · docker/docker-ce · GitHub	MISC	gith
oss-security - CVE-2019-0204: Some Mesos components can be overwritten making arbitrary code execution possible.	MLIST	www
Docker Container Escape ≈ Packet Storm	MISC	pack
GitHub - Frichetten/CVE-2019-5736-PoC: PoC for CVE-2019-5736	MISC	gith
oss-security - Re: runc: CVE-2024-21626: high severity container breakout attack		www
Pony Mail!	MLIST	lists
[SECURITY] Fedora 29 Update: python3-lxc-3.0.4-1.fc29 - package-announce - Fedora Mailing-Lists		lists
[SECURITY] Fedora 30 Update: lxcfs-3.0.4-1.fc30 - package-announce - Fedora Mailing-Lists		lists
Synology Inc.	CONFIRM	www
oss-security - Re: linux-distros membership application - Microsoft	MLIST	www
runC: Multiple vulnerabilities (GLSA 202003-21) — Gentoo security	GENTOO	secu
Security bulletins | Kubernetes Engine Documentation | Google Cloud	MISC	clou
Pony Mail!	MLIST	lists
oss-security - Membership application for linux-distros - VMware	MLIST	www
Red Hat Customer Portal	REDHAT	acce
Mesosphere Support	CONFIRM	supp
Opencontainers runc CVE-2019-5736 Local Command Execution Vulnerability	BID	www
[SECURITY] Fedora 29 Update: runc-1.0.0-92.dev.gitc1b8c57.fc29 - package-announce - Fedora Mailing-Lists		lists
Red Hat Customer Portal	REDHAT	acce
Red Hat Customer Portal	REDHAT	acce
CVE Program record	CVE-ORG	www

CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159170 Oracle Enterprise Linux Security Update for runc (ELSA-2021-9203)
- 174971 SUSE Enterprise Linux Security Update for containerd, docker, runc (SUSE-SU-2021:1458-1)
- 377335 Alibaba Cloud Linux Security Update for container-tools:rhel8 (ALINUX3-SA-2022:0110)
- 500371 Alpine Linux Security Update for lxc
- 501238 Alpine Linux Security Update for runc
- 504128 Alpine Linux Security Update for lxc
- 900005 CBL-Mariner Linux Security Update for moby-buildx 0.4.1
- 900053 CBL-Mariner Linux Security Update for runc 1.0.0.rc8
- 903220 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-buildx (4424)
- 940498 AlmaLinux Security Update for container-tools:rhel8 (ALSA-2019:0975)
- 960701 Rocky Linux Security Update for container-tools:rhel8 (RLSA-2019:0975)

© 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 registred 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