



CVE-2018-15664

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

Summary

CVE	CVE-2018-15664
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-23 14:29:00 UTC
Updated	2019-06-25 12:15:00 UTC
Description	In Docker through 18.06.1-ce-rc2, the API endpoints behind the 'docker cp' command are vulnerable to a symlink-exchange

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Docker	Docker	17.06.0-ce	All	All	All
Application	Docker	Docker	17.06.0-ce	rc1	All	All
Application	Docker	Docker	17.06.0-ce	rc2	All	All
Application	Docker	Docker	17.06.0-ce	rc3	All	All
Application	Docker	Docker	17.06.0-ce	rc4	All	All
Application	Docker	Docker	17.06.0-ce	rc5	All	All
Application	Docker	Docker	17.06.1-ce	All	All	All
Application	Docker	Docker	17.06.1-ce	rc1	All	All
Application	Docker	Docker	17.06.1-ce	rc2	All	All
Application	Docker	Docker	17.06.1-ce	rc3	All	All
Application	Docker	Docker	17.06.1-ce	rc4	All	All
Application	Docker	Docker	17.06.2-ce	All	All	All
Application	Docker	Docker	17.06.2-ce	rc1	All	All
Application	Docker	Docker	17.07.0-ce	All	All	All
Application	Docker	Docker	17.07.0-ce	rc1	All	All
Application	Docker	Docker	17.07.0-ce	rc2	All	All
Application	Docker	Docker	17.07.0-ce	rc3	All	All

Application	Docker	Docker	17.07.0-ce	rc4	All	All
Application	Docker	Docker	17.09.0-ce	All	All	All
Application	Docker	Docker	17.09.0-ce	rc1	All	All
Application	Docker	Docker	17.09.0-ce	rc2	All	All
Application	Docker	Docker	17.09.0-ce	rc3	All	All
Application	Docker	Docker	17.09.1-ce	All	All	All
Application	Docker	Docker	17.09.1-ce-	rc1	All	All
Application	Docker	Docker	17.10.0-ce	All	All	All
Application	Docker	Docker	17.10.0-ce	rc1	All	All
Application	Docker	Docker	17.10.0-ce	rc2	All	All
Application	Docker	Docker	17.11.0-ce	All	All	All
Application	Docker	Docker	17.11.0-ce	rc1	All	All
Application	Docker	Docker	17.11.0-ce	rc2	All	All
Application	Docker	Docker	17.11.0-ce	rc3	All	All
Application	Docker	Docker	17.11.0-ce	rc4	All	All
Application	Docker	Docker	17.12.0-ce	All	All	All
Application	Docker	Docker	17.12.0-ce	rc1	All	All
Application	Docker	Docker	17.12.0-ce	rc2	All	All
Application	Docker	Docker	17.12.0-ce	rc3	All	All
Application	Docker	Docker	17.12.0-ce	rc4	All	All
Application	Docker	Docker	17.12.1-ce	All	All	All
Application	Docker	Docker	17.12.1-ce	rc1	All	All
Application	Docker	Docker	17.12.1-ce	rc2	All	All
Application	Docker	Docker	18.01.0-ce	All	All	All
Application	Docker	Docker	18.01.0-ce	rc1	All	All
Application	Docker	Docker	18.02.0-ce	All	All	All
Application	Docker	Docker	18.02.0-ce	rc1	All	All
Application	Docker	Docker	18.02.0-ce	rc2	All	All
Application	Docker	Docker	18.03.0-ce	All	All	All
Application	Docker	Docker	18.03.0-ce	rc1	All	All
Application	Docker	Docker	18.03.0-ce	rc2	All	All
Application	Docker	Docker	18.03.0-ce	rc3	All	All
Application	Docker	Docker	18.03.0-ce	rc4	All	All
Application	Docker	Docker	18.03.1-ce	All	All	All
Application	Docker	Docker	18.03.1-ce	rc1	All	All

Application	Docker	Docker	17.09.1-ce-	rc1	All	All
Application	Docker	Docker	17.10.0-ce	All	All	All
Application	Docker	Docker	17.10.0-ce	rc1	All	All
Application	Docker	Docker	17.10.0-ce	rc2	All	All
Application	Docker	Docker	17.11.0-ce	All	All	All
Application	Docker	Docker	17.11.0-ce	rc1	All	All
Application	Docker	Docker	17.11.0-ce	rc2	All	All
Application	Docker	Docker	17.11.0-ce	rc3	All	All
Application	Docker	Docker	17.11.0-ce	rc4	All	All
Application	Docker	Docker	17.12.0-ce	All	All	All
Application	Docker	Docker	17.12.0-ce	rc1	All	All
Application	Docker	Docker	17.12.0-ce	rc2	All	All
Application	Docker	Docker	17.12.0-ce	rc3	All	All
Application	Docker	Docker	17.12.0-ce	rc4	All	All
Application	Docker	Docker	17.12.1-ce	All	All	All
Application	Docker	Docker	17.12.1-ce	rc1	All	All
Application	Docker	Docker	17.12.1-ce	rc2	All	All
Application	Docker	Docker	18.01.0-ce	All	All	All
Application	Docker	Docker	18.01.0-ce	rc1	All	All
Application	Docker	Docker	18.02.0-ce	All	All	All
Application	Docker	Docker	18.02.0-ce	rc1	All	All
Application	Docker	Docker	18.02.0-ce	rc2	All	All
Application	Docker	Docker	18.03.0-ce	All	All	All
Application	Docker	Docker	18.03.0-ce	rc1	All	All
Application	Docker	Docker	18.03.0-ce	rc2	All	All
Application	Docker	Docker	18.03.0-ce	rc3	All	All
Application	Docker	Docker	18.03.0-ce	rc4	All	All
Application	Docker	Docker	18.03.1-ce	All	All	All
Application	Docker	Docker	18.03.1-ce	rc1	All	All
Application	Docker	Docker	18.03.1-ce	rc2	All	All
Application	Docker	Docker	18.04.0-ce	All	All	All
Application	Docker	Docker	18.04.0-ce	rc1	All	All
Application	Docker	Docker	18.04.0-ce	rc2	All	All
Application	Docker	Docker	18.05.0-ce	All	All	All
Application	Docker	Docker	18.05.0-ce	rc1	All	All
Application	Docker	Docker	18.06.0-ce	All	All	All

Application	Docker	Docker	18.06.0-ce	rc1	All	All
Application	Docker	Docker	18.06.0-ce	rc2	All	All
Application	Docker	Docker	18.06.0-ce	rc3	All	All
Application	Docker	Docker	18.06.1-ce	rc1	All	All
Application	Docker	Docker	18.06.1-ce	rc2	All	All

References

Reference	Source
Bug 1096726 – VUL-0: CVE-2018-15664: docker: 'docker cp' is vulnerable to symlink-exchange race attacks	MISC
Red Hat Customer Portal	REDHAT
oss-security - RE: CVE-2018-15664: docker (all versions) is vulnerable to a symlink-race attack	MLIST
[security-announce] openSUSE-SU-2019:2044-1: moderate: Security update f	SUSE
[security-announce] openSUSE-SU-2019:1621-1: moderate: Security update f	SUSE
USN-4048-1: Docker vulnerabilities Ubuntu security notices Ubuntu	UBUNTU
Docker CVE-2018-15664 Symlink Directory Traversal Vulnerability	BID
Footer Resource links	CONFIRM
daemon: archive: pause containers before doing filesystem operations by cyphar · Pull Request #39252 · moby/moby · GitHub	MISC
oss-security - CVE-2018-15664: docker (all versions) is vulnerable to a symlink-race attack	MLIST
CVE-2018-15664 - Red Hat Customer Portal	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

353054 Amazon Linux Security Advisory for docker : ALAS2NITRO-ENCLAVES-2021-004
353067 Amazon Linux Security Advisory for docker : ALAS2DOCKER-2021-004
500864 Alpine Linux Security Update for docker
504668 Alpine Linux Security Update for docker

© 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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report