



CVE-2018-1000400

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

Summary

CVE	CVE-2018-1000400
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-18 18:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Kubernetes CRI-O version prior to 1.9 contains a Privilege Context Switching Error (CWE-270) vulnerability in the handling

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kubernetes	Cri-o	All	All	All	All
Application	Kubernetes	Cri-o	All	All	All	All

References

Reference	Source	Link	Tags
[1.9] Remove ambient capabilities by mrunalp · Pull Request #1558 · cri-o/cri-o · GitHub	MISC	github.com	Patch, Third Party
Kubernetes CRI-O CVE-2018-1000400 Remote Privilege Escalation Vulnerability	BID	www.securityfocus.com	Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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