



CVE-2023-6476

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

Summary

CVE	CVE-2023-6476
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-01-09 22:15:00 UTC
Updated	2024-02-04 20:15:00 UTC
Description	Description unavailable.

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	4.13	All	All	All
Application	Redhat	Openshift Container Platform	4.14	All	All	All

References

Reference	Source	Link
cve-details		access.re
Red Hat		access.re
2253994 – (CVE-2023-6476) CVE-2023-6476 cri-o: Pods are able to break out of resource confinement on cgroupv2		bugzilla.r
Red Hat		access.re
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy OID Mappings

[242712](#) Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2024:0195)

[770221](#) Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2024:0207)

[770222](#) Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2024:0195)

© [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](#)