



CVE-2022-4318

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-4318
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-25 20:15:00 UTC
Updated	2023-11-07 03:57:00 UTC
Description	A vulnerability was found in cri-o. This issue allows the addition of arbitrary lines into /etc/passwd by use of a specially crafted

Risk And Classification

Problem Types: CWE-913

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fedoraproject	Extra Packages For Enterprise Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Kubernetes	Cri-o	-	All	All	All
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 For Arm64	4.11	All	All	All
Application	Redhat	Openshift Container Platform For Arm64	4.12	All	All	All
Application	Redhat	Openshift Container Platform For Linuxone	4.11	All	All	All
Application	Redhat	Openshift Container Platform For Linuxone	4.12	All	All	All
Application	Redhat	Openshift Container Platform For Power	4.11	All	All	All
Application	Redhat	Openshift Container Platform For Power	4.12	All	All	All
Application	Redhat	Openshift Container Platform Ibm Z Systems	4.11	All	All	All
Application	Redhat	Openshift Container Platform Ibm Z Systems	4.12	All	All	All

References

Reference	Source	Link	Tags
-----------	--------	------	------

Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
2152703 – (CVE-2022-4318) CVE-2022-4318 cri-o: /etc/passwd tampering privesc	MISC	bugzilla.redhat.com	
cve-details	MISC	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

241241 Red Hat OpenShift Container Platform 4.12 Security Update (RHSA-2023:1033)
241311 Red Hat OpenShift Container Platform 4.11 Security Update (RHSA-2023:1503)
770179 Red Hat OpenShift Container Platform 4.12 Security Update (RHSA-2023:1033)
770182 Red Hat OpenShift Container Platform 4.11 Security Update (RHSA-2023:1503)

© [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