



CVE-2022-27649

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

Summary

CVE	CVE-2022-27649
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-04 20:15:00 UTC
Updated	2023-11-07 03:45:00 UTC
Description	A flaw was found in Podman, where containers were started incorrectly with non-empty default permissions. A vulnerability

Risk And Classification

Problem Types: CWE-276

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Operating System	Fedoraproject	Fedora	34	All
Operating System	Fedoraproject	Fedora	35	All
Operating System	Fedoraproject	Fedora	36	All
Application	Podman Project	Podman	All	All
Application	Redhat	Developer Tools	1.0	All
Operating System	Redhat	Enterprise Linux	8.0	All
Operating System	Redhat	Enterprise Linux	8.6	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.6	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.4	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.6	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	8.4	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All
Operating System	Redhat	Enterprise Linux Server Aus	8.6	All

Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	8.4	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	8.6	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All
Operating System	Redhat	Enterprise Linux Server Tus	8.6	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	8.4	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	8.6	All
Application	Redhat	Openshift Container Platform	4.0	All

References

Reference	Source	L
Default inheritable capabilities for linux container should be empty · Advisory · containers/podman · GitHub	MISC	gi
[SECURITY] Fedora 35 Update: podman-3.4.7-1.fc35 - package-announce - Fedora Mailing-Lists		lic
[SECURITY] Fedora 35 Update: podman-3.4.7-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lic
do not set the inheritable capabilities · containers/podman@aafa809 · GitHub	MISC	gi
[SECURITY] Fedora 36 Update: podman-4.0.3-1.fc36 - package-announce - Fedora Mailing-Lists		lic
[SECURITY] Fedora 34 Update: podman-3.4.7-1.fc34 - package-announce - Fedora Mailing-Lists		lic
2066568 – (CVE-2022-27649) CVE-2022-27649 podman: Default inheritable capabilities for linux container should be empty	MISC	br
[SECURITY] Fedora 36 Update: podman-4.0.3-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lic
[SECURITY] Fedora 34 Update: podman-3.4.7-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lic
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159769](#) Oracle Enterprise Linux Security Update for container-tools:2.0 (ELSA-2022-1566)

[159772](#) Oracle Enterprise Linux Security Update for container-tools:3.0 (ELSA-2022-1565)

[159829](#) Oracle Enterprise Linux Security Update for container-tools:ol8 (ELSA-2022-1762)

[184501](#) Debian Security Update for libpod (CVE-2022-27649)

[240218](#) Red Hat Update for container-tools:2.0 (RHSA-2022:1407)

[240238](#) Red Hat Update for container-tools:2.0 (RHSA-2022:1566)

[240240](#) Red Hat Update for container-tools:3.0 (RHSA-2022:1565)

[240293](#) Red Hat Update for container-tools:rhel8 security (RHSA-2022:1762)

240354 Red Hat Update for container-tools:2.0 (RHSA-2022:4651)
240387 Red Hat Update for container-tools:3.0 (RHSA-2022:4816)
282631 Fedora Security Update for podman (FEDORA-2022-c87047f163)
282683 Fedora Security Update for podman (FEDORA-2022-5e637f6cc6)
377411 Alibaba Cloud Linux Security Update for container-tools:3.0 (ALINUX3-SA-2022:0033)
502156 Alpine Linux Security Update for podman
502335 Alpine Linux Security Update for podman
753592 SUSE Enterprise Linux Security Update for podman (SUSE-SU-2023:0187-1)
753659 SUSE Enterprise Linux Security Update for podman (SUSE-SU-2023:0326-1)
900882 Common Base Linux Mariner (CBL-Mariner) Security Update for podman (9320)
902616 Common Base Linux Mariner (CBL-Mariner) Security Update for podman (9320-1)
940486 AlmaLinux Security Update for container-tools:3.0 (ALSA-2022:1565)
940487 AlmaLinux Security Update for container-tools:2.0 (ALSA-2022:1566)
940562 AlmaLinux Security Update for container-tools:rhel8 (ALSA-2022:1762)
960194 Rocky Linux Security Update for container-tools:rhel8 (RLSA-2022:1762)
960216 Rocky Linux Security Update for container-tools:2.0 (RLSA-2022:1566)
960279 Rocky Linux Security Update for container-tools:3.0 (RLSA-2022:1565)

© [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](#)