



# CVE-2021-20199

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

## Summary

<b>CVE</b>	CVE-2021-20199
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-02-02 19:15:00 UTC
<b>Updated</b>	2021-02-26 03:32:00 UTC
<b>Description</b>	Rootless containers run with Podman, receive all traffic with a source IP address of 127.0.0.1 (including from remote hosts)

## Risk And Classification

**Problem Types:** CWE-346

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Podman Project</a>	Podman	All	All	All	All
Application	<a href="#">Podman Project</a>	Podman	All	All	All	All

## References

Reference	Source
port: add ChildIP by giuseppe · Pull Request #206 · rootless-containers/rootlesskit · GitHub	MISC
1919050 – (CVE-2021-20199) CVE-2021-20199 podman: Remote traffic to rootless containers is seen as originating from localhost	MISC
Source IP always 127.0.0.1 in rootless Podman 1.8.0 · Issue #5138 · containers/podman · GitHub	MISC
rootlessport: set source IP to slirp4netns device by giuseppe · Pull Request #9052 · containers/podman · GitHub	MISC
CVE Program record	CVE.OF
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159458](#) Oracle Enterprise Linux Security Update for container-tools:ol8 (ELSA-2021-1796)

[160293](#) Oracle Enterprise Linux Security Update for podman (ELSA-2022-7954)

180303 Debian Security Update for rootlesskitlibpod (CVE-2021-20199)
239301 Red Hat Update for container-tools:rhel8 (RHSA-2021:1796)
240876 Red Hat Update for podman (RHSA-2022:7954)
501897 Alpine Linux Security Update for podman
751822 OpenSUSE Security Update for common, libcontainers-common, libseccomp, podman (openSUSE-SU-2022:23018-1)
752014 SUSE Enterprise Linux Security Update for common, libcontainers-common, libseccomp, podman (SUSE-SU-2022:23018-1)
752601 SUSE Enterprise Linux Security Update for libcontainers-common (SUSE-SU-2022:3312-1)
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)
901065 Common Base Linux Mariner (CBL-Mariner) Security Update for podman (7329)
902632 Common Base Linux Mariner (CBL-Mariner) Security Update for podman (7329-1)
940208 AlmaLinux Security Update for container-tools:rhel8 (ALSA-2021:1796)
940834 AlmaLinux Security Update for podman (ALSA-2022:7954)
960349 Rocky Linux Security Update for container-tools:rhel8 (RLSA-2021:1796)
982548 Go (go) Security Update for github.com/containers/podman/v3 (GHSA-grh6-q6m2-rh72)

© [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](#)**