CVE-2019-10152

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-10152
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-30 23:15:00 UTC
Updated	2020-09-30 14:11:00 UTC
Description	A path traversal vulnerability has been discovered in podman before version 1.4.0 in the way it handles symlinks inside con

Risk And Classification

Problem Types: CWE-22 | CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libpod Project	Libpod	All	All	All	All
Application	Libpod Project	Libpod	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference
podman/RELEASE_NOTES.md at master · containers/podman · GitHub
[security-announce] openSUSE-SU-2019:2044-1: moderate: Security update f
Resolve symlinks in cp by mheon · Pull Request #3214 · containers/podman · GitHub
Podman cp dereferences symlinks in host context · Issue #3211 · containers/podman · GitHub
1715667 – (CVE-2019-10152) CVE-2019-10152 podman: Improper symlink resolution allows access to host files when executing `podman cp
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report