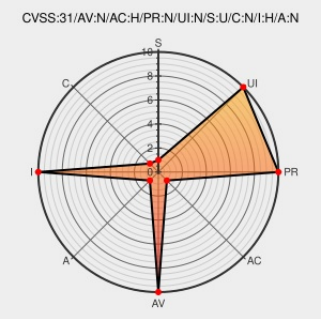
CVE-2020-1726

Published on: 02/11/2020 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:40:00 PM UTC

CVE-2020-1726

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Libpod from Libpod Project contain the following vulnerability:

A flaw was discovered in Podman where it incorrectly allows containers when created to overwrite existing files in volumes, even if they are mounted as read-only. When a user runs a malicious container or a container based on a malicious image with an attached volume that is used for the first time, it is possible to trigger the flaw and overwrite files in the volume.This issue was introduced in version 1.6.0.

CVE-2020-1726 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **The** - **podman** version **= from 1.6.0 onwards**

CVSS3 Score: 5.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link

1801152 – (CVE-2020-1726) CVE-2020-1726 podman: incorrectly allows existing files in volumes to be overwritten by a container when it is created	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1726
[security-announce] openSUSE-SU-2020:1559-1: moderate: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:1559
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2020-1726
1801152 – (CVE-2020-1726) CVE-2020-1726 podman: incorrectly allows existing files in volumes to be overwritten by a container when it is created	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1801152
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2020:0680
[security-announce] openSUSE-SU-2020:1552-1: moderate: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:1552
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2020:1650

Related QID Numbers

159667 Oracle Enterprise Linux Security Update for container-tools:ol8 (ELSA-2020-1650)

377377 Alibaba Cloud Linux Security Update for container-tools:rhel8 (ALINUX3-SA-2021:0013)

501895 Alpine Linux Security Update for podman

750618 OpenSUSE Security Update for conmon, fuse-overlayfs, libcontainers-common, podman (openSUSE-SU-2020:1559-1)

750623 OpenSUSE Security Update for conmon, fuse-overlayfs, libcontainers-common, podman (openSUSE-SU-2020:1552-1)

770014 Red Hat OpenShift Container Platform 4.3.5 Security Update (RHSA-2020:0680)

940531 AlmaLinux Security Update for container-tools:rhel8 (ALSA-2020:1650)

960829 Rocky Linux Security Update for container-tools:rhel8 (RLSA-2020:1650)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libpod Project	Libpod	1.6.0	-	All	All
Application	Libpod Project	Libpod	1.6.0	-	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

Application	Redhat	Openshift Container Platform	4.3	All	All	All
Application	Redhat	Openshift Container Platform	4.3	All	All	All

cpe:2.3:a:libpod_project:libpod:1.6.0:-:*:*:*:*:*:*:

cpe:2.3:a:libpod_project:libpod:1.6.0:-:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→