CVE-2022-1708

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-1708
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-07 18:15:00 UTC
Updated	2023-07-24 13:31:00 UTC
Description	A vulnerability was found in CRI-O that causes memory or disk space exhaustion on the node for anyone with access to the

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Kubernetes	Cri-o	All	All	All	All
Application	Kubernetes	Cri-o	1.24.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	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	3.11	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Redhat	Openshift Container Platform	4.10	All	All	All
Application	Redhat	Openshift Container Platform	4.9	All	All	All

References

Reference	Source	Link
Merge pull request from GHSA-fcm2-6c3h-pg6j · cri-o/cri-o@f032cf6 · GitHub	MISC	github.com
2085361 – (CVE-2022-1708) CVE-2022-1708 cri-o: memory exhaustion on the node when access to the kube api	MISC	bugzilla.redh
Node DOS by way of memory exhaustion through ExecSync request · Advisory · cri-o/cri-o · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org

NVD vulnerability detail NVD nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160047 Oracle Enterprise Linux Security Update for cri-o (ELSA-2022-9717)

160048 Oracle Enterprise Linux Security Update for cri-o (ELSA-2022-9719)

160049 Oracle Enterprise Linux Security Update for cri-o (ELSA-2022-9718)

160050 Oracle Enterprise Linux Security Update for cri-o (ELSA-2022-9720)

160213 Oracle Enterprise Linux Security Update for container-tools:4.0 (ELSA-2022-7469)

160233 Oracle Enterprise Linux Security Update for container-tools:ol8 (ELSA-2022-7457)

160237 Oracle Enterprise Linux Security Update for container-tools:3.0 (ELSA-2022-7529)

240464 Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2022:4943)

240465 Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2022:4972)

240472 Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2022:4965)

240475 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2022:4951)

240478 Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2022:4947)

240482 Red Hat OpenShift Container Platform 5 Security Update (RHSA-2022:4999)

240821 Red Hat Update for container-tools:3.0 (RHSA-2022:7529)

240829 Red Hat Update for container-tools:rhel8 security (RHSA-2022:7457)

240847 Red Hat Update for container-tools:4.0 (RHSA-2022:7469)

752769 SUSE Enterprise Linux Security Update for conmon (SUSE-SU-2022:3896-1)

753058 SUSE Enterprise Linux Security Update for conmon (SUSE-SU-2022:4607-1)

753077 SUSE Enterprise Linux Security Update for conmon (SUSE-SU-2022:4635-1)

770155 Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:4943)

770156 Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2022:4972)

770157 Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2022:4965)

770158 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2022:4951)

770159 Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2022:4947)

940773 AlmaLinux Security Update for container-tools:3.0 (ALSA-2022:7529)

940774 AlmaLinux Security Update for container-tools:4.0 (ALSA-2022:7469)

960172 Rocky Linux Security Update for container-tools:rhel8 (RLSA-2022:7457)

960188 Rocky Linux Security Update for container-tools:4.0 (RLSA-2022:7469)

960603 Rocky Linux Security Update for container-tools:3.0 (RLSA-2022:7529)