



CVE-2020-10749

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-10749
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-03 14:15:00 UTC
Updated	2023-11-07 03:14:00 UTC
Description	A vulnerability was found in all versions of containernetworking/plugins before version 0.8.6, that allows malicious container

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cncf	Cni Network Plugins	All	All	All	All
Application	Cncf	Cni Network Plugins	All	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Linuxfoundation	Cni Network Plugins	All	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	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All

References

Reference

- [SECURITY] Fedora 32 Update: golang-github-containernetworking-plugins-0.9.0-1.fc32 - package-announce - Fedora Mailing-Lists
- [security-announce] openSUSE-SU-2020:1050-1: moderate: Security update f
- 1833220 – (CVE-2020-10749) CVE-2020-10749 containernetworking/plugins: IPv6 router advertisements allow for MitM attacks on IPv4 clust
- [security-announce] openSUSE-SU-2020:1049-1: moderate: Security update f

Google Groups

[SECURITY] Fedora 32 Update: golang-github-containernetworking-plugins-0.9.0-1.fc32 - package-announce - Fedora Mailing-Lists

Google Groups

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159645](#) Oracle Enterprise Linux Security Update for container-tools:ol8 (ELSA-2020-4694)

[377858](#) Kubernetes kubelet Internet Protocol (IPv4) Clusters Susceptible Vulnerability

[501592](#) Alpine Linux Security Update for k3s

[752819](#) SUSE Enterprise Linux Security Update for cni-plugins (SUSE-SU-2022:4151-1)

[770027](#) Red Hat OpenShift Container Platform 4.4.8 Security Update (RHSA-2020:2403)

[770031](#) Red Hat OpenShift Container Platform 4.2.36 Security Update (RHSA-2020:2592)

[770077](#) Red Hat OpenShift Container Platform 4.3 Security Update (RHSA-2020:2443)

[940550](#) AlmaLinux Security Update for container-tools:rhel8 (ALSA-2020:4694)

[960700](#) Rocky Linux Security Update for container-tools:rhel8 (RLSA-2020:4694)

© [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](#)