



Red Hat Product Errata    RHSA-2024:4672 - Security Advisory

# RHSA-2024:4672 - Security Advisory

Issued: 2024-07-22    Updated: 2024-07-22

[Overview](#)[Updated Packages](#)

## Synopsis

Important: containernetworking-plugins security update

## Type/Severity

Security Advisory: Important

### Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) 

## Topic

An update for containernetworking-plugins is now available for Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

## Description

The Container Network Interface (CNI) project consists of a specification and libraries for writing plug-ins for configuring network interfaces in Linux containers, along with a number of supported plug-ins. CNI concerns itself only with network connectivity of containers and removing allocated resources when the container is deleted.

Security Fix(es):

- [golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads \(CVE-2024-1394\)](#)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

## Solution


For details on how to apply this update, which includes the changes described in this advisory, refer to:

<https://access.redhat.com/articles/11258> 

## Affected Products

- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 9.0 x86\_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x

## Fixes

- [BZ - 2262921](#)  - CVE-2024-1394 [golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads](#)

## CVEs

- [CVE-2024-1394](#) 

## References

- <https://access.redhat.com/security/updates/classification/#important> 

---

The Red Hat security contact is [secalert@redhat.com](mailto:secalert@redhat.com). More contact details at <https://access.redhat.com/security/team/contact/>.



Quick Links



Help




Site Info



Related Sites



 Loading



[About Red Hat](#)

[Jobs](#)

[Events](#)

[Locations](#)

[Contact Red Hat](#)

[Red Hat Blog](#)

[Inclusion at Red Hat](#)

[Cool Stuff Store](#)

[Red Hat Summit](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

All policies and guidelines

Digital accessibility

Cookie Preferences and Opt-Out Rights