



Red Hat Product Errata RHSA-2024:1502 - Security Advisory

RHSA-2024:1502 - Security Advisory

Issued: 2024-03-25 Updated: 2024-03-25

[Overview](#)

[Updated Packages](#)

Synopsis

Important: grafana-pcp 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 grafana-pcp is now available for Red Hat Enterprise Linux 9.

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

grafana-pcp is an open source Grafana plugin for PCP.

Security Fix(es):

- grafana-pcp: golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads (CVE-2024-1394)

Solution

Before applying this update, make sure all previously released errata relevant to your system have been applied.

For details on how to apply this update, refer to:

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

Affected Products

- Red Hat Enterprise Linux for x86_64 9 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat Enterprise Linux Server - AUS 9.6 x86_64
- Red Hat Enterprise Linux Server - AUS 9.4 x86_64
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat Enterprise Linux for ARM 64 9 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x

- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x

Fixes

(none)

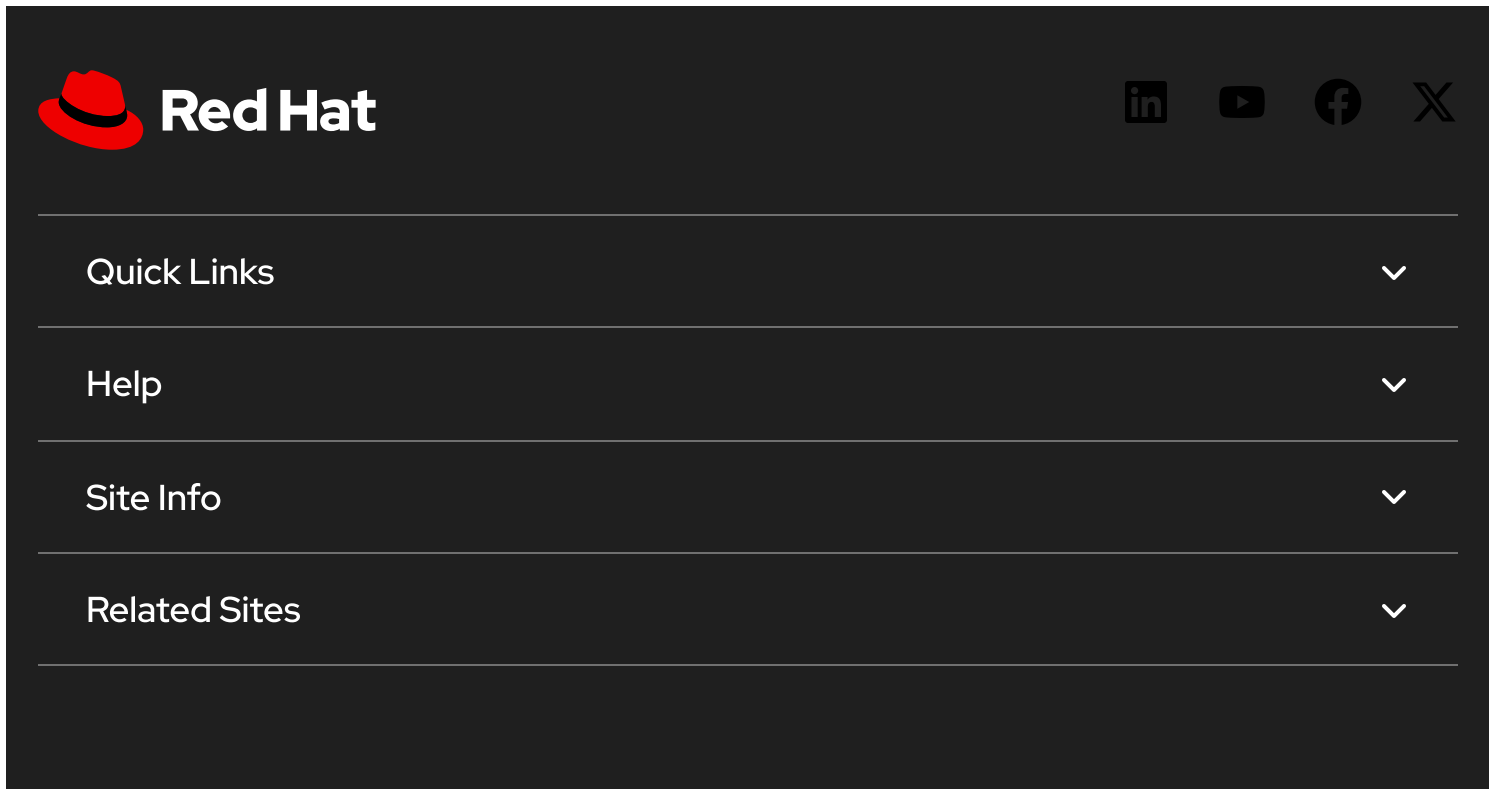
CVEs

- CVE-2024-1394 [↗](#)


References

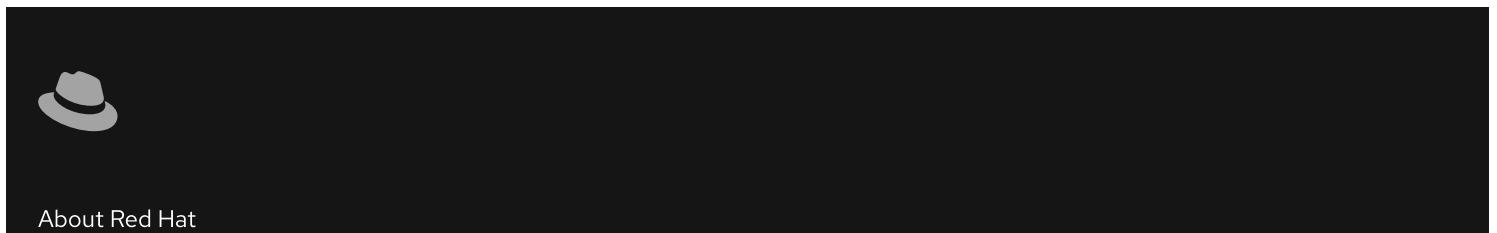
- <https://access.redhat.com/security/updates/classification/#important> [↗](#)

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



The image shows a dark-themed navigation bar for the Red Hat website. On the left is the Red Hat logo, consisting of a red fedora hat icon and the text "Red Hat" in white. On the right are four social media icons: LinkedIn, YouTube, Facebook, and X. Below the logo and icons is a vertical list of navigation items, each with a white downward-pointing chevron icon to its right: "Quick Links", "Help", "Site Info", and "Related Sites".

 Partial system outage



The image shows a dark-themed footer section. On the left is a small, light-colored fedora hat icon. To its right is the text "About Red Hat" in a light color.

[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](#)