



Red Hat Product Errata    RHSA-2024:1646 - Security Advisory

# RHSA-2024:1646 - Security Advisory

Issued: 2024-04-02    Updated: 2024-04-02

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

## Synopsis

Important: grafana security and bug fix 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 is now available for Red Hat Enterprise Linux 8.

'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 is an open source, feature rich metrics dashboard and graph editor for Graphite, InfluxDB & OpenTSDB.

Security Fix(es):

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

Bug Fix(es):

- TRIAGE CVE-2024-1394 grafana: golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads (JIRA:RHEL-30543)

## 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 for x86\_64 8 x86\_64
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat Enterprise Linux for x86\_64 - Extended Life Cycle 8.10 x86\_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 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](#)