



Red Hat Product Errata    RHSA-2026:10708 - Security Advisory

# RHSA-2026:10708 - Security Advisory

Issued: 2026-04-27    Updated: 2026-04-27

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

## Synopsis

Important: gdk-pixbuf2 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 gdk-pixbuf2 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

The gdk-pixbuf2 packages provide an image loading library that can be extended by loadable modules for new image formats. It is used by toolkits such as GTK+ or clutter.

Security Fix(es):

- gdk-pixbuf: gdk-pixbuf: Denial of Service via heap-based buffer overflow when processing a specially crafted JPEG image (CVE-2026-5201)

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 for x86\_64 9 x86\_64
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for ARM 64 9 aarch64

## Fixes

- [BZ - 2453291](#)  - CVE-2026-5201 gdk-pixbuf: gdk-pixbuf: Denial of Service via heap-based buffer overflow when processing a specially crafted JPEG image

## CVEs

- [CVE-2026-5201](#) 

## 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



 Partial system outage



[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