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

Keywords: Security

Status: NEW

Alias: CVE-2026-5201

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2026-03-31 07:23 UTC by OSIDB Bzimport

Modified: 2026-03-31 08:26 UTC (History)

CC List: 0 users

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-03-31 07:23:34 UTC Description

```
Heap-Based Buffer Overflow vulnerability in the JPEG image
loader of the gdk-pixbuf library. The flaw is caused by
improper validation of color component counts in the
gdk_pixbuf__jpeg_image_load() function, leading to
insufficient memory allocation for pixel data. When a
specially crafted JPEG image is processed, libjpeg writes more
data than allocated, resulting in a heap buffer overflow. This
can be triggered automatically via thumbnail generation
without user interaction, causing application crashes and
denial-of-service conditions. Claims of code execution are not
reliably substantiated and require unrealistic conditions;
however, the memory corruption and crash impact are confirmed
```

```
with high confidence.
```

Note

You need to log in before you can comment on or make changes to this bug.