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: 2026-04-28 07:12 UTC (History)

CC List: 0 users

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2026:10707	0	None	None	None	2026-04-27 01:34:18 UTC
Red Hat Product Errata	RHSA-2026:10708	0	None	None	None	2026-04-27 02:01:49 UTC

Red Hat Product Errata	RHSA-2026:10741	0	None	None	None	2026-04-27 09:06:12 UTC
Red Hat Product Errata	RHSA-2026:11325	0	None	None	None	2026-04-28 06:57:52 UTC
Red Hat Product Errata	RHSA-2026:11326	0	None	None	None	2026-04-28 07:03:45 UTC
Red Hat Product Errata	RHSA-2026:11327	0	None	None	None	2026-04-28 07:07:38 UTC
Red Hat Product Errata	RHSA-2026:11328	0	None	None	None	2026-04-28 07:12:04 UTC

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.

errata-xmlrpc 2026-04-27 01:34:17 UTC Comment 2

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 10

Via RHSA-2026:10707 https://access.redhat.com/errata/RHSA-2026:10707

errata-xmlrpc 2026-04-27 02:01:48 UTC Comment 3

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2026:10708 https://access.redhat.com/errata/RHSA-2026:10708

errata-xmlrpc 2026-04-27 09:06:11 UTC Comment 4

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2026:10741 https://access.redhat.com/errata/RHSA-2026:10741

errata-xmlrpc 2026-04-28 06:57:52 UTC Comment 5

This issue has been addressed in the following products:

Red Hat Enterprise Linux 10.0 Extended Update Support

Via RHSA-2026:11325 https://access.redhat.com/errata/RHSA-2026:11325

errata-xmlrpc 2026-04-28 07:03:44 UTC Comment 6

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.2 Update Services for SAP Solutions

Via RHSA-2026:11326 https://access.redhat.com/errata/RHSA-2026:11326

errata-xmlrpc 2026-04-28 07:07:37 UTC Comment 7

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.6 Extended Update Support

Via RHSA-2026:11327 https://access.redhat.com/errata/RHSA-2026:11327

errata-xmlrpc 2026-04-28 07:12:03 UTC Comment 8

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2026:11328 https://access.redhat.com/errata/RHSA-2026:11328

Note

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