Bug 2419093 (CVE-2025-14087) - CVE-2025-14087 glib: GLib: Buffer underflow in GVariant parser leads to heap corruption

Keywords: Security

Status: NEW

Alias: CVE-2025-14087

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: ~~2419097~~ ~~2419098~~ ~~2419099~~ ~~2419100~~ ~~2419101~~ ~~2419102~~ ~~2419103~~ ~~2419104~~ ~~2419105~~ ~~2419106~~ ~~2419107~~ ~~2419108~~ ~~2419109~~ ~~2419111~~ ~~2419112~~ ~~2419113~~ ~~2419114~~ ~~2419115~~ ~~2419116~~ ~~2419117~~ ~~2419118~~ ~~2419119~~ ~~2419120~~ ~~2419121~~ ~~2419122~~ ~~2419123~~ ~~2419124~~ ~~2419125~~ ~~2419126~~ ~~2419127~~ ~~2419128~~ ~~2419129~~ ~~2419130~~ ~~2419131~~ ~~2419132~~ ~~2419133~~ ~~2419134~~

Blocks:

TreeView+ depends on / blocked

Reported: 2025-12-05 08:44 UTC by OSIDB Bzimport

Modified: 2026-03-10 11:52 UTC (History)

CC List: 6 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2025-12-05 08:44:36 UTC Description

A buffer-underflow vulnerability exists in GLib’s GVariant parser, specifically within bytestring_parse() and string_parse(). The parser uses signed 32-bit integers (gint) as loop indices (i and j). When extremely large strings are parsed, these counters overflow into negative values, causing the parser to write to memory before the start of the allocated buffer (str[j++]). This results in a classic out-of-bounds write condition. Because GVariant parsing is often performed on attacker-influenced data, a remote attacker can trigger heap corruption, causing a crash or potentially achieving code execution. This flaw has been confirmed by maintainers and patched upstream.

lmigso 2026-02-11 09:26:01 UTC Comment 1

The current state per RHEL's advisory for CVE-2025-14087 is Fix Deferred. Is there an ETA for when this will be patched, particularly as the CVE has been rated by NVD as Critical.

Note

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