Bug 2429886 (CVE-2026-0988) - CVE-2026-0988 glib: GLib: Denial of Service via Integer Overflow in g_buffered_input_stream_peek()

Keywords: Security ×

Status: NEW

Alias: CVE-2026-0988

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: low

Severity: low

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: ~~2429888~~ ~~2429889~~ ~~2429890~~ ~~2429891~~ ~~2429892~~ ~~2429893~~ ~~2429894~~ ~~2429895~~ ~~2429896~~ ~~2429897~~ ~~2429898~~ ~~2429899~~ ~~2429900~~ ~~2429901~~ ~~2429902~~ ~~2429903~~ ~~2429904~~ ~~2429905~~ ~~2429906~~ ~~2429907~~ ~~2429908~~ ~~2429909~~ ~~2429910~~ ~~2429911~~ ~~2429912~~ ~~2429913~~ ~~2429914~~ ~~2429915~~ ~~2429916~~ ~~2429917~~ ~~2429918~~ ~~2429919~~ ~~2429920~~ ~~2429921~~ ~~2429922~~ ~~2429923~~

Blocks:

TreeView+ depends on / blocked

Reported: 2026-01-15 11:26 UTC by OSIDB Bzimport

Modified: 2026-01-21 11:25 UTC (History)

CC List: 5 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-01-15 11:26:11 UTC Description

```
Integer Overflow vulnerability in the
g_buffered_input_stream_peek() function of the GLib library.
```

The issue is caused by missing validation of the offset and count parameters, leading to an unsafe arithmetic operation during length calculation. When specially crafted values are provided, the offset + count computation may overflow, resulting in an incorrect size being passed to memcpy(). This can trigger a heap or stack buffer overflow and lead to a segmentation fault. Exploitation is subject to strict preconditions and primarily impacts availability by causing application crashes.

Note

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