



## Bug 2421339 (CVE-2025-14512) - CVE-2025-14512 glib: Integer Overflow in GLib GIO Attribute Escaping Causes Heap Buffer Overflow

**Keywords:** Security

**Reported:** 2025-12-11 06:30 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2025-12-18 05:42 UTC ([History](#))

**Alias:** CVE-2025-14512

**CC List:** 0 users

**Product:** Security Response

**Component:** vulnerability

**Fixed In Version:**

**Clone Of:**

**Version:** unspecified

**Environment:**

**Hardware:** All

**Last Closed:**

**OS:** Linux

**Embargoed:**

**Priority:** medium

**Severity:** medium

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:** [2421342](#) [2421343](#) [2421344](#)  
[2421345](#)

**Blocks:**

**TreeView+** [depends on](#) / [blocked](#)

**Attachments** ([Terms of Use](#))

OSIDB Bzimport  2025-12-11 06:30:14 UTC[Description](#)

This vulnerability stems from an integer overflow in GLib's GIO `escape_byte_string()` function, where the count of invalid characters is multiplied using a signed integer, resulting in a too-small memory allocation for escaped output. When a malicious file or remote filesystem supplies attribute values with a large number of invalid bytes, the subsequent escaping loop writes beyond the allocated buffer, triggering a heap buffer overflow and crashing the process.

---

**Note**

You need to [log in](#) before you can comment on or make changes to this bug.

