



# Glib: integer overflow in glib gio attribute escaping causes heap buffer overflow

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2025-14512
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-12-11 07:16:00 UTC
<b>Updated</b>	2026-04-19 20:16:20 UTC
<b>Description</b>	A flaw was found in glib. This vulnerability allows a heap buffer overflow and denial-of-service (DoS) via an integer overflow

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from secalert@redhat.com

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

**EPSS:** 0.000720000 probability, percentile 0.218710000 (date 2026-04-19)

**Problem Types:** CWE-190 | CWE-190 Integer Overflow or Wraparound

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnome	Glib	All	All	All	All
Operating System	Redhat	Enterprise Linux	10.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Openshift	4.0	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GNOME	Glib	affected 2.86.3 semver	Not specified
CNA	Red Hat	Red Hat Hardened Images	unaffected 2.88.0-1.1.hum1 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified

### References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Tracking, Third Party Advisory
gitlab.gnome.org/GNOME/glib/-/issues/3845	secalert@redhat.com	gitlab.gnome.org	
access.redhat.com/security/cve/CVE-2025-14512	secalert@redhat.com	access.redhat.com	Third Party Advisory
access.redhat.com/errata/RHSA-2026:7461	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical

## Vendor Comments And Credit

## Discovery Credit

**CNA:** Red Hat would like to thank Codean Labs for reporting this issue. (en)

## Additional Advisory Data

Source	Time	Event
CNA	2025-12-11T06:22:59.701Z	Reported to Red Hat.
CNA	2025-12-11T00:00:00.000Z	Made public.

## Workarounds

**CNA:** Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base, or stability.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)