Glib: glib: buffer underflow in gvariant parser leads to heap corruption

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-14087
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-10 09:15:47 UTC
Updated	2026-04-19 20:16:20 UTC
Description	A flaw was found in GLib (Gnome Lib). This vulnerability allows a remote attacker to cause heap corruption, leading to a de

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.002840000 probability, percentile 0.518810000 (date 2026-04-19)

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

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	secalert@redhat.com	Secondary	5.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	CVSS	5.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

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 10	Not specified	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 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 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 Enterprise Linux 9	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified

References

References

Reference	Source	Link	Tags
gitlab.gnome.org/GNOME/glib/-/issues/3834	secalert@redhat.com	gitlab.gnome.org	
access.redhat.com/errata/RHSA-2026:7461	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Tracking, Third Party Advisory
access.redhat.com/security/cve/CVE-2025-14087	secalert@redhat.com	access.redhat.com	Mitigation, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Sovereign Tech Resilience program (Sovereign Tech Agency) and treeplus for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-12-05T08:35:24.744Z	Reported to Red Hat.
CNA	2025-12-05T00:00:00.000Z	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.