Glib: integer overflow in in g_escape_uri_string()

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

Summary

CVE	CVE-2025-13601
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-11-26 15:15:51 UTC
Updated	2026-04-19 20:16:19 UTC
Description	A heap-based buffer overflow problem was found in glib through an incorrect calculation of buffer size in the g_escape_uri_

Risk And Classification

Primary CVSS: v3.1 7.7 HIGH from secalert@redhat.com

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

EPSS: 0.000110000 probability, percentile 0.012870000 (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	7.7	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
3.1	CNA	CVSS	7.7	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/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
Application	Redhat	Ceph Storage	8.0	All	All	All
Application	Redhat	Codeready Linux Builder	9.0	All	All	All
Application	Redhat	Codeready Linux Builder For Arm64	10.0	All	All	All
Application	Redhat	Codeready Linux Builder For Arm64	8.0	All	All	All
Application	Redhat	Codeready Linux Builder For Arm64	9.6	All	All	All
Application	Redhat	Codeready Linux Builder For Arm64 Eus	10.0	All	All	All
Application	Redhat	Codeready Linux Builder For Arm64 Eus	9.4	All	All	All
Application	Redhat	Codeready Linux Builder For Ibm Z Systems	10.0_s390x	All	All	All
Application	Redhat	Codeready Linux Builder For Ibm Z Systems	8.0_s390x	All	All	All
Application	Redhat	Codeready Linux Builder For Ibm Z Systems	9.0_s390x	All	All	All
Application	Redhat	Codeready Linux Builder For Ibm Z Systems	9.4_s390x	All	All	All
Application	Redhat	Codeready Linux Builder For Ibm Z Systems	9.6_s390x	All	All	All
Application	Redhat	Codeready Linux Builder For Ibm Z Systems Eus	10.0_s390x	All	All	All
Application	Redhat	Codeready Linux Builder For Power Little Endian	10.0_ppc64le	All	All	All
Application	Redhat	Codeready Linux Builder For Power Little Endian	8.0_ppc64le	All	All	All
Application	Redhat	Codeready Linux Builder For Power Little Endian	9.0_ppc64le	All	All	All
Application	Redhat	Codeready Linux Builder For Power Little Endian	9.4_ppc64le	All	All	All
Application	Redhat	Codeready Linux Builder For Power Little Endian	9.6_ppc64le	All	All	All
Application	Redhat	Codeready Linux Builder For Power Little Endian Eus	10.0_ppc64le	All	All	All
Application	Redhat	Codeready Linux Builder For X86 64	10.0	All	All	All
Application	Redhat	Codeready Linux Builder For X86 64	8.0	All	All	All
Application	Redhat	Codeready Linux Builder For X86 64	9.0	All	All	All
Application	Redhat	Codeready Linux Builder For X86 64	9.4	All	All	All
Application	Redhat	Codeready Linux Builder For X86 64	9.6	All	All	All
Application	Redhat	Codeready Linux Builder For X86 64 Eus	10.0	All	All	All
Application	Redhat	Discovery	2.0	All	All	All
Operating System	Redhat	Enterprise Linux For Arm 64	10.0	All	All	All
Operating System	Redhat	Enterprise Linux For Arm 64	8.0	All	All	All

Operating System	Redhat	Enterprise Linux For Arm 64	9.0	All	All	All
Operating System	Redhat	Enterprise Linux For Arm 64	9.2	All	All	All
Operating System	Redhat	Enterprise Linux For Arm 64	9.4	All	All	All
Operating System	Redhat	Enterprise Linux For Arm 64	9.6	All	All	All
Operating System	Redhat	Enterprise Linux For Arm 64 Eus	10.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	10.0_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	9.0_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	9.2_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	9.4_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	9.6_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	10.0_s390x	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	10.0_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	9.0_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	9.2_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	9.4_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	9.6_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	10.0_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	9.6_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux For X86 64	10.0	All	All	All
Operating System	Redhat	Enterprise Linux For X86 64	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For X86 64	8.6	All	All	All
Operating System	Redhat	Enterprise Linux For X86 64	8.8	All	All	All
Operating System	Redhat	Enterprise Linux For X86 64	9.0	All	All	All
Operating System	Redhat	Enterprise Linux For X86 64	9.2	All	All	All
Operating System	Redhat	Enterprise Linux For X86 64	9.4	All	All	All
Operating System	Redhat	Enterprise Linux For X86 64	9.6	All	All	All
Operating System	Redhat	Enterprise Linux For X86 64 Eus	10.0	All	All	All
Operating System	Redhat	Enterprise Linux For X86 64 Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux For X86 64 Eus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux For X86 64 Eus	8.8	All	All	All
Operating System	Redhat	Enterprise Linux For X86 64 Eus	9.4	All	All	All
Operating System	Redhat	Enterprise Linux For X86 64 Eus	9.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.2	All	All	All

Operating System	Redhat	Enterprise Linux Server Aus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	9.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	9.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	9.6	All	All	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian	10.0_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian	8.6_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian	8.8_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian	9.4_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian	9.6_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Eus	9.4_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.8	All	All	All
Application	Redhat	Openshift Container Platform	4.12	All	All	All
Application	Redhat	Openshift Container Platform	4.16	All	All	All
Application	Redhat	Openshift Container Platform	4.17	All	All	All
Application	Redhat	Openshift Container Platform	4.18	All	All	All
Application	Redhat	Openshift Container Platform	4.19	All	All	All
Application	Redhat	Openshift Container Platform For Arm64	4.12	All	All	All
Application	Redhat	Openshift Container Platform For Arm64	4.16	All	All	All
Application	Redhat	Openshift Container Platform For Arm64	4.17	All	All	All
Application	Redhat	Openshift Container Platform For Arm64	4.18	All	All	All
Application	Redhat	Openshift Container Platform For Arm64	4.19	All	All	All
Application	Redhat	Openshift Container Platform For Ibm Z	4.12	All	All	All
Application	Redhat	Openshift Container Platform For Ibm Z	4.16	All	All	All
Application	Redhat	Openshift Container Platform For Ibm Z	4.17	All	All	All
Application	Redhat	Openshift Container Platform For Ibm Z	4.18	All	All	All
Application	Redhat	Openshift Container Platform For Ibm Z	4.19	All	All	All
Application	Redhat	Openshift Container Platform For Linuxone	4.12	All	All	All
Application	Redhat	Openshift Container Platform For Linuxone	4.16	All	All	All
Application	Redhat	Openshift Container Platform For Linuxone	4.17	All	All	All
Application	Redhat	Openshift Container Platform For Linuxone	4.18	All	All	All
Application	Redhat	Openshift Container Platform For Linuxone	4.19	All	All	All
Application	Redhat	Openshift Container Platform For Power	4.12	All	All	All
Application	Redhat	Openshift Container Platform For Power	4.16	All	All	All

Application	Redhat	Openshift Container Platform For Power	4.17	All	All	All
Application	Redhat	Openshift Container Platform For Power	4.18	All	All	All
Application	Redhat	Openshift Container Platform For Power	4.19	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:2.80.4-10.el10_1.12 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 10.0 Extended Update Support	unaffected 0:2.80.4-4.el10_0.8 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 7 Extended Lifecycle Support	unaffected 0:2.56.1-11.el7_9 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:2.56.4-168.el8_10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 0:2.56.4-8.el8_2.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 0:2.56.4-10.el8_4.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On	unaffected 0:2.56.4-10.el8_4.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 0:2.56.4-158.el8_6.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 0:2.56.4-158.el8_6.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 0:2.56.4-158.el8_6.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Telecommunications Update Service	unaffected 0:2.56.4-164.el8_8 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions	unaffected 0:2.56.4-164.el8_8 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:2.68.4-18.el9_7.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:2.68.4-18.el9_7.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:2.68.4-5.el9_0.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:2.68.4-7.el9_2.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:2.68.4-14.el9_4.5 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.6 Extended Update Support	unaffected 0:2.68.4-16.el9_6.4 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.12	unaffected 412.86.202602021310-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.13	unaffected 413.92.202602240113-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.14	unaffected 414.92.202602171627-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.15	unaffected 415.92.202603101737-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.16	unaffected 416.94.202602101357-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.17	unaffected 417.94.202602090846-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.18	unaffected 418.94.202602022246-0 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.19	unaffected 4.19.9.6.202602112047-0 * rpm
CNA	Red Hat	Red Hat Ceph Storage 8	unaffected sha256:09aaeba975aa74bdf95c
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:519d4fe184cebe5152f8
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:26bb49a8e2e695d6119
CNA	Red Hat	Red Hat Hardened Images	unaffected 2.88.0-1.1.hum1 * rpm

CNA	Red Hat	Red Hat Insights Proxy 1.5	unaffected sha256:975a1e501a8520df83f3
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:83e8b356eb4697a81ff8
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:409a64405669fd11ad87
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:48cf7cf48dfadb17f9357
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:df709663b581b740006c
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:2064	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:1608	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:2659	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:1652	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:2072	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:1465	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:2485	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:1736	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:1624	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:1324	secalert@redhat.com	access.redhat.com	Vendor Advisory
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Tracking, Vendor Advisory
access.redhat.com/errata/RHSA-2026:1627	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:1327	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:3415	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:0975	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:1323	secalert@redhat.com	access.redhat.com	Vendor Advisory
gitlab.gnome.org/GNOME/glib/-/merge_requests/4914	secalert@redhat.com	gitlab.gnome.org	Third Party Advisory
gitlab.gnome.org/GNOME/glib/-/issues/3827	secalert@redhat.com	gitlab.gnome.org	Exploit, Issue Tracking
access.redhat.com/errata/RHSA-2026:0936	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:0991	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:2671	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:1326	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:1626	secalert@redhat.com	access.redhat.com	Vendor Advisory

access.redhat.com/errata/RHSA-2026:7461	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:2563	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/security/cve/CVE-2025-13601	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:4419	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:2974	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:2633	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:1625	secalert@redhat.com	access.redhat.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-11-24T12:49:28.274Z	Reported to Red Hat.
CNA	2025-11-24T13:00:15.295Z	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.