Glib: buffer underflow on glib through glib/gstring.c via function g_string_insert_unichar

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

Summary

CVE	CVE-2025-4373
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-05-06 15:16:05 UTC
Updated	2026-05-12 13:17:21 UTC
Description	A flaw was found in GLib, which is vulnerable to an integer overflow in the g_string_insert_unichar() function. When the pos

Risk And Classification

Primary CVSS: v3.1 4.8 MEDIUM from secalert@redhat.com

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

EPSS: 0.007420000 probability, percentile 0.730900000 (date 2026-05-12)

Problem Types: CWE-124 | CWE-124 Buffer Underwrite ('Buffer Underflow')

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L
3.1	CNA	CVSS	4.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:2.80.4-4.el10_0.6 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:2.56.4-166.el8_10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.2 Advanced Update Support	unaffected 0:2.56.4-8.el8_2.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support	unaffected 0:2.56.4-10.el8_4.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On	unaffected 0:2.56.4-10.el8_4.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support	unaffected 0:2.56.4-158.el8_6.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Telecommunications Update Service	unaffected 0:2.56.4-158.el8_6.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions	unaffected 0:2.56.4-158.el8_6.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Telecommunications Update Service	unaffected 0:2.56.4-162.el8_8 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions	unaffected 0:2.56.4-162.el8_8 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:2.68.4-16.el9_6.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:2.68.4-16.el9_6.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:2.68.4-5.el9_0.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:2.68.4-7.el9_2.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:2.68.4-14.el9_4.3 * rpm
CNA	Red Hat	Red Hat Insights Proxy 1.5	unaffected sha256:e54a5a5f9d69dd6a03e2
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.6.0	unaffected sha256:a891aa3f77d70d9d796
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.6.0	unaffected sha256:d9ca4a9ec5bc8de23e4
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.6.0	unaffected sha256:addf7b49ce99777a3bbf
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.6.0	unaffected sha256:d4ef54ac8de0eaf22e29
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.6.0	unaffected sha256:1c4617b035c66b6b34e
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.6.0	unaffected sha256:8c5dddd29d08fe8234ec
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.6.0	unaffected sha256:be3feca3b19ac609e5ef
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.6.0	unaffected sha256:3d37f30462f237f5087ef
CNA	Red Hat	Red Hat OpenShift Distributed Tracing 3.6.0	unaffected sha256:8fb68adefecd8ccb9440
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified

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 7	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.3 custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	affected V3.3 custom
ADP	Siemens	SCALANCE XCH328	affected V3.3 custom
ADP	Siemens	SCALANCE XCM324	affected V3.3 custom
ADP	Siemens	SCALANCE XCM328	affected V3.3 custom
ADP	Siemens	SCALANCE XCM332	affected V3.3 custom
ADP	Siemens	SCALANCE XRH334 24 V DC 8xFO CC	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 230 V AC 12xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 230 V AC 8xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 230V AC 2x10G 24xSFP 8xSFP	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 24 V DC 12xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 24 V DC 8xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 24V DC 2x10G 24xSFP 8xSFP	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 2x230 V AC 12xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 2x230 V AC 8xFO	affected V3.3 custom
ADP	Siemens	SCALANCE XRM334 2x230V AC 2x10G 24xSFP 8xSFP	affected V3.3 custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2025:10855	secalert@redhat.com	access.redhat.com	
gitlab.gnome.org/GNOME/glib/-/issues/3677	secalert@redhat.com	gitlab.gnome.org	
access.redhat.com/security/cve/CVE-2025-4373	secalert@redhat.com	access.redhat.com	

cert-portal.siemens.com/productcert/html/ssa-089022.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
access.redhat.com/errata/RHSA-2025:12275	secalert@redhat.com	access.redhat.com	
cert-portal.siemens.com/productcert/html/ssa-082556.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
access.redhat.com/errata/RHSA-2025:11662	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:11374	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:11327	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:13335	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:14989	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:11373	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:14988	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:11140	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:14990	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/errata/RHSA-2025:14991	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-05-06T00:33:30.003Z	Reported to Red Hat.
CNA	2025-05-06T00:00:00.000Z	Made public.

Workarounds

CNA: Currently, no mitigation is available for this vulnerability.

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