



# CVE-2024-34397

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

## Summary

<b>CVE</b>	CVE-2024-34397
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-05-07 18:15:08 UTC
<b>Updated</b>	2026-05-12 12:16:35 UTC
<b>Description</b>	An issue was discovered in GNOME GLib before 2.78.5, and 2.79.x and 2.80.x before 2.80.1. When a GDBus-based client

## Risk And Classification

**Primary CVSS:** v3.1 5.2 MEDIUM from ADP

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

**Problem Types:** CWE-290 | n/a | CWE-290 CWE-290 Authentication Bypass by Spoofing

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	5.2	MEDIUM	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.2	MEDIUM	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L

## CVSS v3.1 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

Low

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnome	Glib	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.1 custom	Not specified
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * custom	Not specified
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	affected V3.1 custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified

### References

Reference	Source	Link
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...	af854a3a-2127-422b-91ae-364da2661108	lists.f...
lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/mess...	af854a3a-2127-422b-91ae-364da2661108	lists.f...
cert-portal.siemens.com/productcert/html/ssa-082556.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-p...
gitlab.gnome.org/GNOME/glib/-/issues/3268	af854a3a-2127-422b-91ae-364da2661108	gitlab...
lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/mess...	af854a3a-2127-422b-91ae-364da2661108	lists.f...
lists.debian.org/debian-lts-announce/2024/05/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.d...
www.openwall.com/lists/oss-security/2024/05/07/5	af854a3a-2127-422b-91ae-364da2661108	www....
cert-portal.siemens.com/productcert/html/ssa-613116.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-p...
security.netapp.com/advisory/ntap-20240531-0008	af854a3a-2127-422b-91ae-364da2661108	secur...
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...	af854a3a-2127-422b-91ae-364da2661108	lists.f...
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...	af854a3a-2127-422b-91ae-364da2661108	lists.f...
lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/mess...	af854a3a-2127-422b-91ae-364da2661108	lists.f...
lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/mess...	af854a3a-2127-422b-91ae-364da2661108	lists.f...
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...	af854a3a-2127-422b-91ae-364da2661108	lists.f...
CVE Program record	CVE.ORG	www....

No vendor comments have been submitted for this CVE.

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](#)