



# gpib: lpvo\_usb: fix memory leak on disconnect

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-31760
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-01 15:16:39 UTC
<b>Updated</b>	2026-05-08 18:11:51 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: gpib: lpvo_usb: fix memory leak on disconnect The driver

## Risk And Classification

**Primary CVSS:** v3.1 5.5 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.000170000 probability, percentile 0.040610000 (date 2026-05-05)

**Problem Types:** CWE-401

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected fce79512a96afacbe297ba3c5c2f7ed34944540d 21f942879f86108b300a23683e67483f8c358fc7 git
CNA	Linux	Linux	affected fce79512a96afacbe297ba3c5c2f7ed34944540d 706f4fe2dacc95d65e7c8dff321711f024bb8d20 git
CNA	Linux	Linux	affected fce79512a96afacbe297ba3c5c2f7ed34944540d 5cefb52c1af6f69ea719e42788f6ec6a087eb74c git
CNA	Linux	Linux	affected 6.13
CNA	Linux	Linux	unaffected 6.13 semver
CNA	Linux	Linux	unaffected 6.18.22 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.12 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

## References

Reference	Source	Link	Tags
git.kernel.org/stable/c/706f4fe2dacc95d65e7c8dff321711f024bb8d20	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/5cefb52c1af6f69ea719e42788f6ec6a087eb74c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/21f942879f86108b300a23683e67483f8c358fc7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)