



# reset: gpio: fix double free in reset\_add\_gpio\_aux\_device() error path

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

## Summary

<b>CVE</b>	CVE-2026-31745
<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 15:16:37 UTC
<b>Updated</b>	2026-05-07 19:31:28 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: reset: gpio: fix double free in reset\_add\_gpio\_aux\_device()

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from nvd@nist.gov

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

**EPSS:** 0.000150000 probability, percentile 0.029500000 (date 2026-05-12)

**Problem Types:** CWE-415

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	7.0	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	7.0	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	7.0	rc3	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	7.0	rc4	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	7.0	rc5	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	7.0	rc6	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	7.0	rc7	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5fc4e4cf7a2268b5f73700fd1e8d02159f2417d8 1de465753220deb41569cf2add87bbb0673731db git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5fc4e4cf7a2268b5f73700fd1e8d02159f2417d8 fbffb8c7c7bb4d38e9f65e0bee446685011de5d8 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.19
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.12 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original_commit_for_fix

### References

Reference	Source	Link	Tags
<a href="https://git.kernel.org/stable/c/1de465753220deb41569cf2add87bbb0673731db">git.kernel.org/stable/c/1de465753220deb41569cf2add87bbb0673731db</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
<a href="https://git.kernel.org/stable/c/fbffb8c7c7bb4d38e9f65e0bee446685011de5d8">git.kernel.org/stable/c/fbffb8c7c7bb4d38e9f65e0bee446685011de5d8</a>	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>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

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