



# usb: gadget: f\_rndis: Fix net\_device lifecycle with device\_move

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

## Summary

<b>CVE</b>	CVE-2026-31722
<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 15:16:34 UTC
<b>Updated</b>	2026-05-06 20:55:31 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f\_rndis: Fix net\_device lifecycle with device\_

## 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:** 0.000180000 probability, percentile 0.046430000 (date 2026-05-05)

**Problem Types:** NVD-CWE-noinfo

## 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 f466c6353819326873fa48a02c6f2d7c903240d6 1ef251aa63972fe6c0f107f5abd139b7d0f7987a git
CNA	Linux	Linux	affected f466c6353819326873fa48a02c6f2d7c903240d6 18ada801899f2b13ef0ceff42427ad980a41e619 git
CNA	Linux	Linux	affected f466c6353819326873fa48a02c6f2d7c903240d6 6045ea5ca6e3fa13f8a9fafb1c535c86e124c14d git
CNA	Linux	Linux	affected f466c6353819326873fa48a02c6f2d7c903240d6 e367599529dc42578545a7f85fde517b35b3cda7 git
CNA	Linux	Linux	affected 3.11
CNA	Linux	Linux	unaffected 3.11 semver
CNA	Linux	Linux	unaffected 6.12.81 6.12.* 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/e367599529dc42578545a7f85fde517b35b3cda7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/18ada801899f2b13ef0ceff42427ad980a41e619	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/6045ea5ca6e3fa13f8a9fafb1c535c86e124c14d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/1ef251aa63972fe6c0f107f5abd139b7d0f7987a	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.

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)