



can: usb: f81604: correctly anchor the urb in the read bulk callback

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-23347 |
| State | PUBLISHED |
| Assigner | Linux |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-03-25 11:16:32 UTC |
| Updated | 2026-04-24 18:10:38 UTC |

Description In the Linux kernel, the following vulnerability has been resolved: can: usb: f81604: correctly anchor the urb in the read bulk

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

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 88da17436973e463bed59bea79771fb03a21555e 54ee74307165b348b2fddcd7942eb48fb4ee1237 g |
| CNA | Linux | Linux | affected 88da17436973e463bed59bea79771fb03a21555e c001214e12202338425d6dda5d2a1919d674282d |
| CNA | Linux | Linux | affected 88da17436973e463bed59bea79771fb03a21555e f6d80b104f904a6da922907394eec66d3e2ffc57 git |
| CNA | Linux | Linux | affected 88da17436973e463bed59bea79771fb03a21555e 7724645c4792914cd07f36718816c5369cc57970 g |
| CNA | Linux | Linux | affected 88da17436973e463bed59bea79771fb03a21555e 952caa5da10bed22be09612433964f6877ba0dde c |
| CNA | Linux | Linux | affected 6.5 |
| CNA | Linux | Linux | unaffected 6.5 semver |
| CNA | Linux | Linux | unaffected 6.6.130 6.6.* semver |
| CNA | Linux | Linux | unaffected 6.12.77 6.12.* semver |
| CNA | Linux | Linux | unaffected 6.18.17 6.18.* semver |
| CNA | Linux | Linux | unaffected 6.19.7 6.19.* semver |
| CNA | Linux | Linux | unaffected 7.0 * original_commit_for_fix |

References

| Reference | Source | Link | Tags |
|--|--------------------------------------|---|---------|
| git.kernel.org/stable/c/54ee74307165b348b2fddcd7942eb48fb4ee1237 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch |
| git.kernel.org/stable/c/952caa5da10bed22be09612433964f6877ba0dde | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch |
| git.kernel.org/stable/c/c001214e12202338425d6dda5d2a1919d674282d | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch |
| git.kernel.org/stable/c/f6d80b104f904a6da922907394eec66d3e2ffc57 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch |
| git.kernel.org/stable/c/7724645c4792914cd07f36718816c5369cc57970 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch |
| CVE Program record | CVE.ORG | www.cve.org | canonic |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonic |

No vendor comments have been submitted for this CVE.

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

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](#)