



rxrpc: proc: size address buffers for %p|SpC output

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-31630 |
| State | PUBLISHED |
| Assigner | Linux |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-24 15:16:42 UTC |
| Updated | 2026-04-24 17:51:40 UTC |

Description In the Linux kernel, the following vulnerability has been resolved: rxrpc: proc: size address buffers for %p|SpC output The Al

Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|--------|-----------------------|-----------------------|--|
| CNA | Linux | Linux | affected 75b54cb57ca34cbe7a87c6ac757c55360a624590 db297c78ce537c9ac96f0eda9b25ad72c8caefa9 git |
| CNA | Linux | Linux | affected 75b54cb57ca34cbe7a87c6ac757c55360a624590 10ebed83f9f6414af4e85bc85ffaeda7effdd874 git |
| CNA | Linux | Linux | affected 75b54cb57ca34cbe7a87c6ac757c55360a624590 a44ce6aa2efb61fe44f2cfab72bb01544bbca272 git |
| CNA | Linux | Linux | affected 4.9 |
| CNA | Linux | Linux | unaffected 4.9 semver |
| CNA | Linux | Linux | unaffected 6.18.23 6.18.* semver |
| CNA | Linux | Linux | unaffected 6.19.13 6.19.* semver |
| CNA | Linux | Linux | unaffected 7.0 * original_commit_for_fix |

References

| Reference | Source | Link | Tags |
|---|--------------------------------------|---|-----------|
| git.kernel.org/stable/c/db297c78ce537c9ac96f0eda9b25ad72c8caefa9 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/a44ce6aa2efb61fe44f2cfab72bb01544bbca272 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/10ebed83f9f6414af4e85bc85ffaeda7effdd874 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | 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](#) 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](#)