



# rxrpc: fix RESPONSE authenticator parser OOB read

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

## Summary

<b>CVE</b>	CVE-2026-31636
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-24 15:16:42 UTC
<b>Updated</b>	2026-04-24 17:51:40 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: rxrpc: fix RESPONSE authenticator parser OOB read rxgp

## Risk And Classification

**EPSS:** 0.000170000 probability, percentile 0.040730000 (date 2026-04-25)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 9d1d2b59341f58126a69b51f9f5f8ccb9f12e54a 7875f3d9777bd4e9892c4db830571ab8ac2044c0 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 9d1d2b59341f58126a69b51f9f5f8ccb9f12e54a 20a188775a9a9982d1987e12660d9b44b40a6c99 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 9d1d2b59341f58126a69b51f9f5f8ccb9f12e54a 3e3138007887504ee9206d0bfb5acb062c600025 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.16
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.16 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.23 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.13 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/20a188775a9a9982d1987e12660d9b44b40a6c99">git.kernel.org/stable/c/20a188775a9a9982d1987e12660d9b44b40a6c99</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/3e3138007887504ee9206d0bfb5acb062c600025">git.kernel.org/stable/c/3e3138007887504ee9206d0bfb5acb062c600025</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/7875f3d9777bd4e9892c4db830571ab8ac2044c0">git.kernel.org/stable/c/7875f3d9777bd4e9892c4db830571ab8ac2044c0</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
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.

© [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](#)