



# rxrpc, afs: Fix missing error pointer check after rxrpc\_kernel\_lookup\_peer()

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

## Summary

<b>CVE</b>	CVE-2026-43463
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-08 15:16:59 UTC
<b>Updated</b>	2026-05-12 14:10:27 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: rxrpc, afs: Fix missing error pointer check after rxrpc\_kern

## Risk And Classification

**EPSS:** 0.000170000 probability, percentile 0.041320000 (date 2026-05-12)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 72904d7b9bfbf2dd146254edea93958bc35bbbfe d55fa7cd4b19ba91b34b307d769c149e56ad0a75 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 72904d7b9bfbf2dd146254edea93958bc35bbbfe 54331c5dcc6d97683d7ca2788e7ef9c9505e1477 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 72904d7b9bfbf2dd146254edea93958bc35bbbfe 4245a79003adf30e67f8e9060915bd05cb31d142 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 056fc740be000d39a7dba700a935f3bbfbc664e6 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.8
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.8 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.19 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.9 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original_commit_for_fix

## References

Reference	Source	Link	Tags
git.kernel.org/stable/c/d55fa7cd4b19ba91b34b307d769c149e56ad0a75	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/54331c5dcc6d97683d7ca2788e7ef9c9505e1477	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/4245a79003adf30e67f8e9060915bd05cb31d142	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonic

CVE Program Home	SEARCH	<a href="http://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="http://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](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**Free CVE JSON API** [cve.report/api](http://cve.report/api)

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