



crypto: algif_aead - Fix minimum RX size check for decryption

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

Summary

CVE	CVE-2026-43077
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 10:16:20 UTC
Updated	2026-05-06 13:08:07 UTC

Description In the Linux kernel, the following vulnerability has been resolved: crypto: algif_aead - Fix minimum RX size check for decryption

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected d887c52d6ae43aeebd249b5f2f1333e60236aa60 74a66fdb5282d89e348b00c42cfca3a936946d94 git
CNA	Linux	Linux	affected d887c52d6ae43aeebd249b5f2f1333e60236aa60 fd427dd84f224309afbcc2cb67c7bb770a01265c git
CNA	Linux	Linux	affected d887c52d6ae43aeebd249b5f2f1333e60236aa60 1c76b5675119f694458293a2a81f40731c69bd32 git
CNA	Linux	Linux	affected d887c52d6ae43aeebd249b5f2f1333e60236aa60 e86ab1e5661386a874fbb8551f0c04b8e9f8ad22 git
CNA	Linux	Linux	affected d887c52d6ae43aeebd249b5f2f1333e60236aa60 af2fa2fbbced26129813274b8b3f7705f280e174 git
CNA	Linux	Linux	affected d887c52d6ae43aeebd249b5f2f1333e60236aa60 78cea133daf721698876e56135049a96d39d610a git
CNA	Linux	Linux	affected d887c52d6ae43aeebd249b5f2f1333e60236aa60 3afdc15d6173614d7d834517d9b65e7aa5a08548 git
CNA	Linux	Linux	affected d887c52d6ae43aeebd249b5f2f1333e60236aa60 3d14bd48e3a77091cbce637a12c2ae31b4a1687c git
CNA	Linux	Linux	affected 4.14
CNA	Linux	Linux	unaffected 4.14 semver
CNA	Linux	Linux	unaffected 5.10.254 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.204 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.170 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.136 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.83 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.24 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.14 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/3afdc15d6173614d7d834517d9b65e7aa5a08548	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/74a66fdb5282d89e348b00c42cfca3a936946d94	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/fd427dd84f224309afbcc2cb67c7bb770a01265c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/3d14bd48e3a77091cbce637a12c2ae31b4a1687c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/af2fa2fbbced26129813274b8b3f7705f280e174	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e86ab1e5661386a874fbb8551f0c04b8e9f8ad22	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/78cea133daf721698876e56135049a96d39d610a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1c76b5675119f694458293a2a81f40731c69bd32	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
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.

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). 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