



af_key: validate families in pfkey_send_migrate()

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2026-31515
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 14:16:50 UTC
Updated	2026-04-22 14:16:50 UTC

Description In the Linux kernel, the following vulnerability has been resolved: af_key: validate families in pfkey_send_migrate() syzbot w

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 08de61beab8a21c8e0b3906a97defda5f1f66ece d0c5aa8dd38887714f1aad04236a3620b56a5e4e git
CNA	Linux	Linux	affected 08de61beab8a21c8e0b3906a97defda5f1f66ece e06b596fc4eb01936a2e5dccad17c946d660bab8 git
CNA	Linux	Linux	affected 08de61beab8a21c8e0b3906a97defda5f1f66ece 8ddf8de7e758f6888988467af9ffc8adf589fb16 git
CNA	Linux	Linux	affected 08de61beab8a21c8e0b3906a97defda5f1f66ece d3225e6b9bd51ec177970a628fe4b11237ce87d5 git
CNA	Linux	Linux	affected 08de61beab8a21c8e0b3906a97defda5f1f66ece 7b18692c59afb8e5c364c8e3ac01e51dd6b52028 git
CNA	Linux	Linux	affected 08de61beab8a21c8e0b3906a97defda5f1f66ece 83f644ea92987c100b82d8481ae2230faeed3d34 git
CNA	Linux	Linux	affected 08de61beab8a21c8e0b3906a97defda5f1f66ece ee836e820a40e2ca4da8af7310bff92d586772d4 git
CNA	Linux	Linux	affected 08de61beab8a21c8e0b3906a97defda5f1f66ece eb2d16a7d599dc9d4df391b5e660df9949963786 git
CNA	Linux	Linux	affected 2.6.21
CNA	Linux	Linux	unaffected 2.6.21 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.168 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.131 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.80 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.21 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.11 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/e06b596fc4eb01936a2e5dccad17c946d660bab8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d0c5aa8dd38887714f1aad04236a3620b56a5e4e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/8ddf8de7e758f6888988467af9ffc8adf589fb16	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d3225e6b9bd51ec177970a628fe4b11237ce87d5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/eb2d16a7d599dc9d4df391b5e660df9949963786	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ee836e820a40e2ca4da8af7310bff92d586772d4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/7b18692c59afb8e5c364c8e3ac01e51dd6b52028	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/83f644ea92987c100b82d8481ae2230faeed3d34	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