



# netfilter: nft\_set\_pipapo\_avx2: don't return non-matching entry on expiry

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

## Summary

<b>CVE</b>	CVE-2026-43114
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 10:16:25 UTC
<b>Updated</b>	2026-05-08 17:54:04 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: netfilter: nft\_set\_pipapo\_avx2: don't return non-matching e

## Risk And Classification

**Primary CVSS:** v3.1 9.4 CRITICAL from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

**EPSS:** 0.000430000 probability, percentile 0.132400000 (date 2026-05-09)

**Problem Types:** NVD-CWE-noinfo

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	9.4	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L
3.1	CNA	DECLARED	9.4	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 7400b063969bdca4a06cd97f1294d765c8eecebe1 fa4f1f52528c73989d820f32bfca06bec5afeece git
CNA	Linux	Linux	affected 7400b063969bdca4a06cd97f1294d765c8eecebe1 3d53f9aafd469ae1ea27051e00f5b96ca1b55d52 git
CNA	Linux	Linux	affected 7400b063969bdca4a06cd97f1294d765c8eecebe1 07de44424bb7f17ef9357e8535df96d9e97c40cb git
CNA	Linux	Linux	affected 7400b063969bdca4a06cd97f1294d765c8eecebe1 0abbc43f71d99baadeeba6fa3fe1c80b676f57ed git
CNA	Linux	Linux	affected 7400b063969bdca4a06cd97f1294d765c8eecebe1 d3c0037ffe1273fa1961e779ff6906234d6cf53c git
CNA	Linux	Linux	affected 5.7
CNA	Linux	Linux	unaffected 5.7 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/d3c0037ffe1273fa1961e779ff6906234d6cf53c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/fa4f1f52528c73989d820f32bfca06bec5afeece	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/0abbc43f71d99baadeeba6fa3fe1c80b676f57ed	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/3d53f9aafd469ae1ea27051e00f5b96ca1b55d52	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/07de44424bb7f17ef9357e8535df96d9e97c40cb	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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](#)