



netfilter: x_tables: restrict xt_check_match/xt_check_target extensions for NFPROTO_ARP

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

Summary

CVE	CVE-2026-31424
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 14:16:12 UTC
Updated	2026-04-18 09:16:32 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: netfilter: x_tables: restrict xt_check_match/xt_check_target

Risk And Classification

EPSS: 0.000240000 probability, percentile 0.066100000 (date 2026-04-18)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 9291747f118d6404e509747b85ff5f6dfec368d2 80e3c75f71c3ea1e62fcb032382de13e00a68f8b git
CNA	Linux	Linux	affected 9291747f118d6404e509747b85ff5f6dfec368d2 d9a0af9e43416aa50c0595e15fa01365a1c72c49 git
CNA	Linux	Linux	affected 9291747f118d6404e509747b85ff5f6dfec368d2 1cd6313c8644bfebbd813a05da9daa21b09dd68c git
CNA	Linux	Linux	affected 9291747f118d6404e509747b85ff5f6dfec368d2 f00ac65c90ea475719e08d629e2e26c8b4e6999b git
CNA	Linux	Linux	affected 9291747f118d6404e509747b85ff5f6dfec368d2 e7e1b6bcb389c8708003d40613a59ff2496f6b1f git
CNA	Linux	Linux	affected 9291747f118d6404e509747b85ff5f6dfec368d2 dc3e27dd7d76e21106b8f9bbdc31f5da74a89014 git
CNA	Linux	Linux	affected 9291747f118d6404e509747b85ff5f6dfec368d2 3e79374b03bf9a2f282f0eb1d0ac3776f7e0f28a git
CNA	Linux	Linux	affected 9291747f118d6404e509747b85ff5f6dfec368d2 3d5d488f11776738deab9da336038add95d342d1 git
CNA	Linux	Linux	affected 2.6.39
CNA	Linux	Linux	unaffected 2.6.39 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 6.6.134 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.81 6.12.* semver

CNA	Linux	Linux	unaffected 6.18.22 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.12 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/dc3e27dd7d76e21106b8f9bbdc31f5da74a89014	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/3d5d488f11776738deab9da336038add95d342d1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/3e79374b03bf9a2f282f0eb1d0ac3776f7e0f28a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d9a0af9e43416aa50c0595e15fa01365a1c72c49	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e7e1b6bcb389c8708003d40613a59ff2496f6b1f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/f00ac65c90ea475719e08d629e2e26c8b4e6999b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/80e3c75f71c3ea1e62fcb032382de13e00a68f8b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1cd6313c8644bfdbbd813a05da9daa21b09dd68c	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). This site includes MITRE data granted under the following [license](https://www.mitre.org).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report