



net: usb: kaweth: remove TX queue manipulation in kaweth_set_rx_mode

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

Summary

CVE	CVE-2026-43180
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:36 UTC
Updated	2026-05-06 13:07:51 UTC

Description In the Linux kernel, the following vulnerability has been resolved: net: usb: kaweth: remove TX queue manipulation in kaweth

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 443a830b1dc4f85c7560da59d4494b629feee215 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 586318c2730433184c6f1d21183e346ddf25e81d git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 a2cd4b4db315a845a5603d08c9d03b11ddfc799d git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 ef9b10a020503888eb6c8ed85a3d901a624ede4c git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 9c79b839a63980c7da7ec5db895198045e154112 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 fc393af769af845d9985e2845e49553d8f015a64 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 8367c0e90126426e60581e4c07e1ec4411a0f843 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 64868f5ecadeb359a49bc4485bfa7c497047f13a git
CNA	Linux	Linux	affected 2.6.12
CNA	Linux	Linux	unaffected 2.6.12 semver
CNA	Linux	Linux	unaffected 5.10.252 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.202 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.165 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.128 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.75 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.16 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/fc393af769af845d9985e2845e49553d8f015a64	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ef9b10a020503888eb6c8ed85a3d901a624ede4c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/586318c2730433184c6f1d21183e346ddf25e81d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/8367c0e90126426e60581e4c07e1ec4411a0f843	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/443a830b1dc4f85c7560da59d4494b629feee215	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a2cd4b4db315a845a5603d08c9d03b11ddfc799d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/64868f5ecadeb359a49bc4485bfa7c497047f13a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9c79b839a63980c7da7ec5db895198045e154112	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