



atm: lec: fix null-ptr-deref in lec_arp_clear_vccs

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

Summary

CVE	CVE-2026-23286
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 11:16:23 UTC
Updated	2026-04-18 09:16:16 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: atm: lec: fix null-ptr-deref in lec_arp_clear_vccs syzkaller r

Risk And Classification

EPSS: 0.000320000 probability, percentile 0.092520000 (date 2026-04-21)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 8aff65a82b6389ec674d46e5b3d3ae6f07db5e3e git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 30c9744a989feb22cfbb84170eb0e038a7a2c1da git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 e9665986eb127290ceb535bd5d04d7a84265d94f git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 622062f24644b4536d3f437e0cf7a8c4bb421665 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 2d9f57ea29a1f1772373b98a509b44d49fda609e git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 7ea92ab075d809ec8a96669a5ecf00f752057875 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 5f1cfea7921f5c126a441d973690eeba52677b64 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 101bacb303e89dc2e0640ae6a5e0fb97c4eb45bb git
CNA	Linux	Linux	affected 2.6.12
CNA	Linux	Linux	unaffected 2.6.12 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 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.77 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.17 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.7 6.19.* semver

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/7ea92ab075d809ec8a96669a5ecf00f752057875	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/5f1cfea7921f5c126a441d973690eeba52677b64	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/8aff65a82b6389ec674d46e5b3d3ae6f07db5e3e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/622062f24644b4536d3f437e0cf7a8c4bb421665	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e9665986eb127290ceb535bd5d04d7a84265d94f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/2d9f57ea29a1f1772373b98a509b44d49fda609e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/101bacb303e89dc2e0640ae6a5e0fb97c4eb45bb	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/30c9744a989feb22cfbb84170eb0e038a7a2c1da	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 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](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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