



# atm: atmtcp: Prevent arbitrary write in atmtcp\_recv\_control().

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

## Summary

<b>CVE</b>	CVE-2025-39828
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-09-16 13:16:03 UTC
<b>Updated</b>	2026-05-12 13:17:14 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: atm: atmtcp: Prevent arbitrary write in atmtcp\_recv\_control().

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from nvd@nist.gov

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

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

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

## 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 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 b502f16bad8f0a4cfbd023452766f21bfda3
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 0a6a6d4fb333f7afe22e59ffed18511a7a98
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 62f368472b0aa4b5d91d9b983152855c6b
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 51872b26429077be611b0a1816e0e7222
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 3c80c230d6e3e6f63d43f4c3f0bb344e3e8
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 33f9e6dc66b32202b95fc861e6b3ea4b0c1
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 3ab9f5ad9baefe6d3d4c37053cdfca27610
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 ec79003c5f9d2c7f9576fc69b8bdba80305
CNA	Linux	Linux	affected 2.6.12
CNA	Linux	Linux	unaffected 2.6.12 semver
CNA	Linux	Linux	unaffected 5.4.298 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.242 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.191 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.150 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.104 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.45 6.12.* semver
CNA	Linux	Linux	unaffected 6.16.5 6.16.* semver
CNA	Linux	Linux	unaffected 6.17 * original_commit_for_fix
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom

## References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org/debian-lts-announce/2025/10/msg00008.html">lists.debian.org</a>
git.kernel.org/stable/c/33f9e6dc66b32202b95fc861e6b3ea4b0c185b0b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/33f9e6dc66b32202b95fc861e6b3ea4b0c185b0b">git.kernel.org</a>
git.kernel.org/stable/c/3ab9f5ad9baefe6d3d4c37053cdfca2761001dfe	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/3ab9f5ad9baefe6d3d4c37053cdfca2761001dfe">git.kernel.org</a>
git.kernel.org/stable/c/ec79003c5f9d2c7f9576fc69b8bdba80305cbe3a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/ec79003c5f9d2c7f9576fc69b8bdba80305cbe3a">git.kernel.org</a>
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com/productcert/html/ssa-032379.html">cert-portal.siemens.cc</a>
git.kernel.org/stable/c/62f368472b0aa4b5d91d9b983152855c6b6d8925	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/62f368472b0aa4b5d91d9b983152855c6b6d8925">git.kernel.org</a>
git.kernel.org/stable/c/0a6a6d4fb333f7afe22e59ffed18511a7a98efc8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/0a6a6d4fb333f7afe22e59ffed18511a7a98efc8">git.kernel.org</a>

<a href="https://git.kernel.org/stable/c/b502f16bad8f0a4cfbd023452766f21bfda39dde">git.kernel.org/stable/c/b502f16bad8f0a4cfbd023452766f21bfda39dde</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/3c80c230d6e3e6f63d43f4c3f0bb344e3e8b119b">git.kernel.org/stable/c/3c80c230d6e3e6f63d43f4c3f0bb344e3e8b119b</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://lists.debian.org/debian-lts-announce/2025/10/msg00007.html">lists.debian.org/debian-lts-announce/2025/10/msg00007.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
<a href="https://git.kernel.org/stable/c/51872b26429077be611b0a1816e0e722278015c3">git.kernel.org/stable/c/51872b26429077be611b0a1816e0e722278015c3</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)