



# tcp\_bpf: fix return value of tcp\_bpf\_sendmsg()

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

## Summary

<b>CVE</b>	CVE-2024-46783
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-09-18 08:15:05 UTC
<b>Updated</b>	2026-05-12 12:17:12 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: tcp\_bpf: fix return value of tcp\_bpf\_sendmsg() When we c

## Risk And Classification

**Primary CVSS:** v3.1 5.5 MEDIUM from nvd@nist.gov

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

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/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 4f738adba30a7cfc006f605707e7aee847ffefc
CNA	Linux	Linux	affected 4f738adba30a7cfc006f605707e7aee847ffefc
CNA	Linux	Linux	affected 4f738adba30a7cfc006f605707e7aee847ffefc
CNA	Linux	Linux	affected 4f738adba30a7cfc006f605707e7aee847ffefc
CNA	Linux	Linux	affected 4f738adba30a7cfc006f605707e7aee847ffefc
CNA	Linux	Linux	affected 4f738adba30a7cfc006f605707e7aee847ffefc
CNA	Linux	Linux	affected 4f738adba30a7cfc006f605707e7aee847ffefc
CNA	Linux	Linux	affected 4.17
CNA	Linux	Linux	unaffected 4.17 semver
CNA	Linux	Linux	unaffected 5.4.284 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.226 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.167 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.110 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.51 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.10 6.10.* semver
CNA	Linux	Linux	unaffected 6.11 * original_commit_for_fix
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.2 custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	affected V3.2 custom
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	affected V3.2 custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

## References

Reference	Source	Link
git.kernel.org/stable/c/3efe53eb221a38e207c1e3f81c51e4ca057d50c2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/78bb38d9c5a311c5f8bdef7c9557d7d81ca30e4a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/810a4e7d92dea4074cb04c25758320909d752193	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
git.kernel.org/stable/c/c8219a27fa43a2cbf99f5176f6dddf73e7a24ae	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/126d72b726c4cf1119f3a7fe413a78d341c3fea9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/fe1910f9337bd46a9343967b547ccab26b4b2c6e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org

git.kernel.org/stable/c/6f9fdf5806cccd888c43512bccbdf7efd50f510	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
lists.debian.org/debian-lts-announce/2024/10/msg00003.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
cert-portal.siemens.com/productcert/html/ssa-355557.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.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)