



# mptcp: make fallback action and fallback decision atomic

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

## Summary

<b>CVE</b>	CVE-2025-38491
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-07-28 12:15:31 UTC
<b>Updated</b>	2026-05-12 13:16:51 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: mptcp: make fallback action and fallback decision atomic

## 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:** CWE-667

## 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	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0530020a7c8f2204e784f0dbdc882bbd961fdbde 5586518bec27666c747cd52aabb62d485
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0530020a7c8f2204e784f0dbdc882bbd961fdbde 75a4c9ab8a7af0d76b31ccd1188ed178c3
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0530020a7c8f2204e784f0dbdc882bbd961fdbde 54999dea879fecb761225e28f274b40662
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0530020a7c8f2204e784f0dbdc882bbd961fdbde 1d82a8fe6ee4afdc92f4e8808c9dad2a609
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0530020a7c8f2204e784f0dbdc882bbd961fdbde f8a1d9b18c5efc76784f5a326e905f641f83
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 609937aa962a62e93acfc04dd370b665e6152dfb git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6654efe264b014d8ea9fc38f79efb568b1b79069 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.19
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.19 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.149 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.101 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.40 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.15.8 6.15.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.16 * original_commit_for_fix
ADP	<a href="#">Siemens</a>	<a href="#">SIMATIC CN 4100</a>	affected V5.0 custom

## References

Reference	Source	Link
<a href="https://lists.debian.org/debian-lts-announce/2025/10/msg00008.html">lists.debian.org/debian-lts-announce/2025/10/msg00008.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/75a4c9ab8a7af0d76b31ccd1188ed178c38b35d2">git.kernel.org/stable/c/75a4c9ab8a7af0d76b31ccd1188ed178c38b35d2</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/f8a1d9b18c5efc76784f5a326e905f641f839894">git.kernel.org/stable/c/f8a1d9b18c5efc76784f5a326e905f641f839894</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/54999dea879fecb761225e28f274b40662918c30">git.kernel.org/stable/c/54999dea879fecb761225e28f274b40662918c30</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/1d82a8fe6ee4afdc92f4e8808c9dad2a6095bbc5">git.kernel.org/stable/c/1d82a8fe6ee4afdc92f4e8808c9dad2a6095bbc5</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://cert-portal.siemens.com/productcert/html/ssa-032379.html">cert-portal.siemens.com/productcert/html/ssa-032379.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.co</a>
<a href="https://git.kernel.org/stable/c/5586518bec27666c747cd52aabb62d485686d0bf">git.kernel.org/stable/c/5586518bec27666c747cd52aabb62d485686d0bf</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](#) 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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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

**CVE.report and Source URL Uptime Status** [status.cve.report](#)