mptcp: make fallback action and fallback decision atomic

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-38491
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-28 12:15:31 UTC
Updated	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 S

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	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 0530020a7c8f2204e784f0dbdc882bbd961fdbde 5586518bec27666c747cd52aabb62d485
CNA	Linux	Linux	affected 0530020a7c8f2204e784f0dbdc882bbd961fdbde 75a4c9ab8a7af0d76b31ccd1188ed178c3
CNA	Linux	Linux	affected 0530020a7c8f2204e784f0dbdc882bbd961fdbde 54999dea879fecb761225e28f274b40662
CNA	Linux	Linux	affected 0530020a7c8f2204e784f0dbdc882bbd961fdbde 1d82a8fe6ee4afdc92f4e8808c9dad2a609
CNA	Linux	Linux	affected 0530020a7c8f2204e784f0dbdc882bbd961fdbde f8a1d9b18c5efc76784f5a326e905f641f83
CNA	Linux	Linux	affected 609937aa962a62e93acfc04dd370b665e6152dfb git
CNA	Linux	Linux	affected 6654efe264b014d8ea9fc38f79efb568b1b79069 git
CNA	Linux	Linux	affected 5.19
CNA	Linux	Linux	unaffected 5.19 semver
CNA	Linux	Linux	unaffected 6.1.149 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.101 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.40 6.12.* semver
CNA	Linux	Linux	unaffected 6.15.8 6.15.* semver
CNA	Linux	Linux	unaffected 6.16 * 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	lists.debian.org
git.kernel.org/stable/c/75a4c9ab8a7af0d76b31ccd1188ed178c38b35d2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/f8a1d9b18c5efc76784f5a326e905f641f839894	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/54999dea879fecb761225e28f274b40662918c30	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/1d82a8fe6ee4afdc92f4e8808c9dad2a6095bbc5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/5586518bec27666c747cd52aabb62d485686d0bf	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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