mptcp: pm: avoid possible UaF when selecting endp

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

Summary

CVE	CVE-2024-44974
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-09-04 20:15:07 UTC
Updated	2026-04-09 17:41:57 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: avoid possible UaF when selecting endp selec

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: CWE-416

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	Debian	Debian Linux	11.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 01cacb00b35cb62b139f07d5f84bcf0eeda8eff6 ddee5b4b6a1cc03c1e9921cf34382e094c2009f1 git
CNA	Linux	Linux	affected 01cacb00b35cb62b139f07d5f84bcf0eeda8eff6 f2c865e9e3ca44fc06b5f73b29a954775e4dbb38 git
CNA	Linux	Linux	affected 01cacb00b35cb62b139f07d5f84bcf0eeda8eff6 2b4f46f9503633dade75cb796dd1949d0e6581a1 git
CNA	Linux	Linux	affected 01cacb00b35cb62b139f07d5f84bcf0eeda8eff6 9a9afbbc3fbfca4975eea4aa5b18556db5a0c0b8 git
CNA	Linux	Linux	affected 01cacb00b35cb62b139f07d5f84bcf0eeda8eff6 0201d65d9806d287a00e0ba96f0321835631f63f git
CNA	Linux	Linux	affected 01cacb00b35cb62b139f07d5f84bcf0eeda8eff6 48e50dcbcbaaf713d82bf2da5c16aeced94ad07d git
CNA	Linux	Linux	affected 5.7
CNA	Linux	Linux	unaffected 5.7 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 6.1.109 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.48 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.7 6.10.* semver
CNA	Linux	Linux	unaffected 6.11 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/48e50dcbcbaaf713d82bf2da5c16aeced94ad07d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/9a9afbbc3fbfca4975eea4aa5b18556db5a0c0b8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/0201d65d9806d287a00e0ba96f0321835631f63f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/f2c865e9e3ca44fc06b5f73b29a954775e4dbb38	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/ddee5b4b6a1cc03c1e9921cf34382e094c2009f1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
lists.debian.org/debian-lts-announce/2024/10/msg00003.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Mailin
git.kernel.org/stable/c/2b4f46f9503633dade75cb796dd1949d0e6581a1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Mailin
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

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**