net/packet: fix TOCTOU race on mmap'd vnet_hdr in tpacket_snd()

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

Summary

CVE	CVE-2026-31700
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 14:16:19 UTC
Updated	2026-05-03 07:16:17 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: net/packet: fix TOCTOU race on mmap'd vnet_hdr in tpac

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000180000 probability, percentile 0.048520000 (date 2026-05-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 1d036d25e5609ba73fee6a88db01c306b140d512 74e2db36fe50e3ad9d5300d7fd0e6e2a15a6d121 gi
CNA	Linux	Linux	affected 1d036d25e5609ba73fee6a88db01c306b140d512 3a1bf9116ea31470b89692585c3910dfe830dcdd gi
CNA	Linux	Linux	affected 1d036d25e5609ba73fee6a88db01c306b140d512 28324a3b62d9ce7f9bdd65a8ce63f382041d1b27 gi
CNA	Linux	Linux	affected 1d036d25e5609ba73fee6a88db01c306b140d512 48a6ef291a17639e1b6ae0fbe9c8b2bb87d7804b gi
CNA	Linux	Linux	affected 1d036d25e5609ba73fee6a88db01c306b140d512 2c054e17d9d41f1020376806c7f750834ced4dc5 gi
CNA	Linux	Linux	affected 4.6
CNA	Linux	Linux	unaffected 4.6 semver
CNA	Linux	Linux	unaffected 6.6.136 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.84 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.25 6.18.* semver
CNA	Linux	Linux	unaffected 7.0.2 7.0.* semver
CNA	Linux	Linux	unaffected 7.1-rc1 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/48a6ef291a17639e1b6ae0fbe9c8b2bb87d7804b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/2c054e17d9d41f1020376806c7f750834ced4dc5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/3a1bf9116ea31470b89692585c3910dfe830dcdd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/74e2db36fe50e3ad9d5300d7fd0e6e2a15a6d121	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/28324a3b62d9ce7f9bdd65a8ce63f382041d1b27	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

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