net: use skb_header_pointer() for TCPv4 GSO frag_off check

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

Summary

CVE	CVE-2026-43036
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 15:16:48 UTC
Updated	2026-05-08 18:44:10 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: net: use skb_header_pointer() for TCPv4 GSO frag_off ch

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

EPSS: 0.000180000 probability, percentile 0.046430000 (date 2026-05-05)

Problem Types: CWE-908

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 cbc53e08a793b073e79f42ca33f1f3568703540d f7a6cd508e9e825a2c69fa9e13d41ee156852f25 git
CNA	Linux	Linux	affected cbc53e08a793b073e79f42ca33f1f3568703540d cc91202fc20a44aab4c206f12a2bfe05da936051 git
CNA	Linux	Linux	affected cbc53e08a793b073e79f42ca33f1f3568703540d d970341cfa5594614c7a6634886c7688b4f5cafd git
CNA	Linux	Linux	affected cbc53e08a793b073e79f42ca33f1f3568703540d ddc748a391dd8642ba6b2e4fe22e7f2ddf84b7f0 git
CNA	Linux	Linux	affected 4.7
CNA	Linux	Linux	unaffected 4.7 semver
CNA	Linux	Linux	unaffected 6.12.81 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.22 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.12 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/d970341cfa5594614c7a6634886c7688b4f5cafd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/f7a6cd508e9e825a2c69fa9e13d41ee156852f25	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/ddc748a391dd8642ba6b2e4fe22e7f2ddf84b7f0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/cc91202fc20a44aab4c206f12a2bfe05da936051	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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