net: correctly handle tunneled traffic on IPV6_CSUM GSO fallback

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

Summary

CVE	CVE-2026-43057
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 15:16:52 UTC
Updated	2026-05-03 07:16:24 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: net: correctly handle tunneled traffic on IPV6_CSUM GSC

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000240000 probability, percentile 0.068220000 (date 2026-05-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected a0478d7e888028f85fa7785ea838ce0ca09398e2 2094a7cf91b71367b649f991aacc7b579f793d0b git
CNA	Linux	Linux	affected 2156d9e9f2e483c8c3906c0ea57ea312c1424235 ed71cf465c75f5688b07a35d373cd1d6b589c8ea git
CNA	Linux	Linux	affected 041e2f945f82fdbd6fff577b79c33469430297aa 33670f780e0120c3dacda188c512bbffe0b6044c git
CNA	Linux	Linux	affected 864e3396976ef41de6cc7bc366276bf4e084fff2 a98b78116a27e2a57b696b569b2cb431c95cf9b6 git
CNA	Linux	Linux	affected 864e3396976ef41de6cc7bc366276bf4e084fff2 732fdeb2987c94b439d51f5cb9addddc2fc48c42 git
CNA	Linux	Linux	affected 864e3396976ef41de6cc7bc366276bf4e084fff2 c4336a07eb6b2526dc2b62928b5104b41a7f81f5 git
CNA	Linux	Linux	affected 794ddbb7b63b6828c75967b9bcd43b086716e7a1 git
CNA	Linux	Linux	affected 6.17
CNA	Linux	Linux	unaffected 6.17 semver
CNA	Linux	Linux	unaffected 6.1.168 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.134 6.6.* 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/ed71cf465c75f5688b07a35d373cd1d6b589c8ea	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a98b78116a27e2a57b696b569b2cb431c95cf9b6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c4336a07eb6b2526dc2b62928b5104b41a7f81f5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/2094a7cf91b71367b649f991aacc7b579f793d0b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/33670f780e0120c3dacda188c512bbffe0b6044c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/732fdeb2987c94b439d51f5cb9addddc2fc48c42	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**