xsk: tighten UMEM headroom validation to account for tailroom and min frame

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

Summary

CVE	CVE-2026-43093
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 10:16:22 UTC
Updated	2026-05-08 13:16:38 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: xsk: tighten UMEM headroom validation to account for tail

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: 0.000120000 probability, percentile 0.017410000 (date 2026-05-11)

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 99e3a236dd43d06c65af0a2ef9cb44306aef6e02 a03975beb9f6af0d8ac051e30b2abeabe618414f git
CNA	Linux	Linux	affected 99e3a236dd43d06c65af0a2ef9cb44306aef6e02 0ec4d3f6e6934deb843b561ae048cd17218e5ad1 git
CNA	Linux	Linux	affected 99e3a236dd43d06c65af0a2ef9cb44306aef6e02 9ea6ba4f3195dcba6e8b3e7b2e748593b7cafb12 git
CNA	Linux	Linux	affected 99e3a236dd43d06c65af0a2ef9cb44306aef6e02 6523bc1b40e69301f24c14338b762af4739d6d39 git
CNA	Linux	Linux	affected 99e3a236dd43d06c65af0a2ef9cb44306aef6e02 a315e022a72d95ef5f1d4e58e903cb492b0ad931 git
CNA	Linux	Linux	affected ad8fb61c184fe0f8d1e0b5b954d010fb9f94a6ee git
CNA	Linux	Linux	affected 25c9cdef57488578da21d99eb614b97ffcf6e59f git
CNA	Linux	Linux	affected 98d3c852e63b49129515dd18c875999efaf8530a git
CNA	Linux	Linux	affected 5.7
CNA	Linux	Linux	unaffected 5.7 semver
CNA	Linux	Linux	unaffected 6.6.136 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.83 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.24 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.14 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/9ea6ba4f3195dcba6e8b3e7b2e748593b7cafb12	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/6523bc1b40e69301f24c14338b762af4739d6d39	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/0ec4d3f6e6934deb843b561ae048cd17218e5ad1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a315e022a72d95ef5f1d4e58e903cb492b0ad931	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a03975beb9f6af0d8ac051e30b2abeabe618414f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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