

CVE-2026-46300

Linux Kernel Missing Initialization of a Variable Vulnerability

CISA KEV since Oct 28, 2026

Actively exploited

Public exploit module (Metasploit)

In the Linux kernel, the following vulnerability has been resolved: net: skbuff: preserve shared-frag marker during coalescing skb_try_coalesce() can attach paged frags from @from to @to. If @from has SKBFL_SHARED_FRAG set, the resulting @to skb can contain the same externally-owned or page-cache-backed frags, but the shared-frag marker is currently lost. That breaks the invariant relied on by later in-place writers.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.102 95.7th percentile · FIRST	CISA DEADLINE Oct 31, 2026 CISA federal deadline in 3 days
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 30 days
☒ EPSS	0.102 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines. **CISA note:** This vulnerability affects an open-source component, third-party library, protocol, or proprietary implementation that could be used by different products. For more information, please see: Basis: CISA KEV required action

In particular, ESP input checks skb_has_shared_frag() before deciding whether an uncloned nonlinear skb can skip skb_cow_data(). If TCP receive coalescing has moved shared frags into an unmarked skb, ESP can see skb_has_shared_frag() as false and decrypt in place over page-cache backed frags. Propagate SKBFL_SHARED_FRAG when skb_try_coalesce() transfers paged frags. The tailroom copy path does not need the marker because it copies bytes into @to's linear data rather than transferring frag descriptors.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
linux kernel	$\geq 3.9 \leq 5.10.257$ $\geq 5.11 < 5.15.208$ $\geq 5.16 < 6.1.174$ $\geq 6.2 < 6.6.141$ $\geq 6.7 < 6.12.91$ $\geq 6.13 < 6.18.33$ $\geq 6.19 < 7.0.10$ 7.1	no fixed version listed	NVD

Sources

Vendor guidance	git.kernel.org/stable/c/2f2b16022a2e10ca7bccfb98db5ed2ec0f72641c	git.kernel.org	git.kernel.org/stable/c/3599e6b3cc1ada96883d496a50a210d3afbb6987
git.kernel.org	git.kernel.org/stable/c/9d3e5fd19fe1063bf607219e8562fbd567b8e8d5	git.kernel.org	git.kernel.org/stable/c/78bf6b6bb19541d19fbda6242e7cfe2c682763c0
git.kernel.org	git.kernel.org/stable/c/760e1addc27ba1a7beb4a0a7e8b3e9ec49e7a34e	git.kernel.org	git.kernel.org/stable/c/3bd9e113d50034db99d7ef69fd8e5242d15e414a
git.kernel.org	git.kernel.org/stable/c/3884358a9286b17f389a72b1426fc4547c23c111	git.kernel.org	git.kernel.org/stable/c/f84eca5817390257cef78013d0112481c503b4a3
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2026-46300	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-31535	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-46300

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.