

CVE-2024-50302

Linux Kernel Use of Uninitialized Resource Vulnerability

CISA KEV since Mar 4, 2025

Actively exploited

In the Linux kernel, the following vulnerability has been resolved: HID: core: zero-initialize the report buffer Since the report buffer is used by all kinds of drivers in various ways, let's zero-initialize it during allocation to make sure that it can't be ever used to leak kernel memory via specially-crafted report.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 5.5 Medium · NVD	EPSS 0.008 56.5th percentile · FIRST	CISA DEADLINE Mar 25, 2025 KEV since 2025 · listed over a year
--	---	---	---

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 two years
☒ EPSS	0.008 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability affects a common open-source component, third-party library, or a protocol used by different products.

Basis: CISA KEV required action

Affected and fixed versions · 26 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
android	–	no fixed version listed	NVD
debian linux	11.0	no fixed version listed	NVD
simatic s7-1500 tm mfp firmware	–	no fixed version listed	NVD
sinec os	< 3.2	no fixed version listed	NVD
linux kernel	≥ 3.12 < 4.19.324 ≥ 4.20 < 5.4.286 ≥ 5.5 < 5.10.230 ≥ 5.11 < 5.15.172 ≥ 5.16 < 6.1.117 ≥ 6.2 < 6.6.61 ≥ 6.7 < 6.11.8 6.12	no fixed version listed	NVD
simatic s7-1500 tm mfp	–	no fixed version listed	NVD
ruggedcom rst2428p	–	no fixed version listed	NVD
scalance xc316-8	–	no fixed version listed	NVD

Sources

Vendor guidance	git.kernel.org/stable/c/05ade5d4337867929e7ef664e7ac8e0c734f1aaf	lore.kernel.org	lore.kernel.org/linux-cve-announce/2024111908-CVE-2024-50302-f677@gregkh/
source.android.com	source.android.com/docs/security/bulletin/2025-03-01	NVD	nvd.nist.gov/vuln/detail/CVE-2024-50302
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-44804
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-50302		

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