

CVE-2025-38352

Linux Kernel Time-of-Check Time-of-Use (TOCTOU) Race Condition Vulnerability

CISA KEV since Sep 4, 2025

Actively exploited

In the Linux kernel, the following vulnerability has been resolved: posix-cpu-timers: fix race between handle_posix_cpu_timers() and posix_cpu_timer_del(). If an exiting non-autoreaping task has already passed exit_notify() and calls handle_posix_cpu_timers() from IRQ, it can be reaped by its parent or debugger right after unlock_task_sighand(). If a concurrent posix_cpu_timer_del() runs at that moment, it won't be able to detect timer->it.cpu.firing != 0: cpu_timer_task_rcu() and/or lock_task_sighand() will fail.

EVRs

75_{/100}

Urgent priority

CVSS V3.1

7.8

High · NVD

EPSS

0.013

71.1st percentile · FIRST

CISA DEADLINE

Sep 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	0.013 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 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. Please check with specific vendors for information on patching status.

Basis: CISA KEV required action

Add the tsk->exit_state check into run_posix_cpu_timers() to fix this. This fix is not needed if CONFIG_POSIX_CPU_TIMERS_TASK_WORK=y, because exit_task_work() is called before exit_notify(). But the check still makes sense, task_work_add(&tsk->posix_cputimers_work.work) will fail anyway in this case.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
linux kernel	≥ 2.6.36 < 5.4.295 ≥ 5.5 < 5.10.239 ≥ 5.11 < 5.15.186 ≥ 5.16 < 6.1.142 ≥ 6.2 < 6.6.94 ≥ 6.7 < 6.12.34 ≥ 6.13 < 6.15.3 6.16	no fixed version listed	NVD
debian linux	11.0	no fixed version listed	NVD

Sources

Vendor guidance	git.kernel.org/stable/c/2c72fe18cc5f9f1750f5bc148cf1c94c29e106ff	git.kernel.org	git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=2c72fe18cc5f9f1750f5bc148cf1c94c29e106ff
source.android.com	source.android.com/docs/security/bulletin/2025-09-01	NVD	nvd.nist.gov/vuln/detail/CVE-2025-38352
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-22297
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-38352		

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