CVE-2013-2094

Linux Kernel Privilege Escalation Vulnerability

CISA KEV since Sep 15, 2022 | Actively exploited

The perf_swevent_init function in kernel/events/core.c in the Linux kernel before 3.8.9 uses an incorrect integer data type, which allows local users to gain privileges via a crafted perf_event_open system call.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
75/100	8.4	0.477	Oct 6, 2022
Urgent priority	High · NVD	98.8th percentile · FIRST	KEV since 2022 · 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	On the CISA KEV catalog for over two years
✓ EPSS	0.477 probability	− Pre-patch disclosure	Disclosure status unavailable
✓ CVSS	Base score 8.4	− Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
linux kernel	< 3.0.75 ⩾ 3.1 < 3.2.45 ⩾ 3.3 < 3.4.42 ⩾ 3.5 < 3.8.9	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-xpgm-72rm-72p4	git.kernel.org	git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8176cced706b5e5d15887584150764894e94e02f
NVD	nvd.nist.gov/vuln/detail/CVE-2013-2094	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2013-2068	Current data	evulnable.com/vulnerability-management/cve/CVE-2013-2094

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