



drm/scheduler: signal scheduled fence when kill job

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2025-38436
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-25 15:15:29 UTC
Updated	2026-04-18 09:16:10 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: drm/scheduler: signal scheduled fence when kill job When

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Problem Types: CWE-667

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected a72ce6f84109c1dec1ab236d65979d3250668af3 8342127a8a65b0673863b106ce32b79c91ae3270 g
CNA	Linux	Linux	affected a72ce6f84109c1dec1ab236d65979d3250668af3 c5734f9bab6f0d40577ad0633af4090a5fda2407 git
CNA	Linux	Linux	affected a72ce6f84109c1dec1ab236d65979d3250668af3 aefd0a935625165a6ca36d0258d2d053901555df git
CNA	Linux	Linux	affected a72ce6f84109c1dec1ab236d65979d3250668af3 aa382a8b6ed483e9812d0e63b6d1bdcba0186f29 gi
CNA	Linux	Linux	affected a72ce6f84109c1dec1ab236d65979d3250668af3 471db2c2d4f80ee94225a1ef246e4f5011733e50 git
CNA	Linux	Linux	affected 4.3
CNA	Linux	Linux	unaffected 4.3 semver
CNA	Linux	Linux	unaffected 6.1.169 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.96 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.36 6.12.* semver
CNA	Linux	Linux	unaffected 6.15.5 6.15.* semver
CNA	Linux	Linux	unaffected 6.16 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/aa382a8b6ed483e9812d0e63b6d1bdcba0186f29	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/c5734f9bab6f0d40577ad0633af4090a5fda2407	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/8342127a8a65b0673863b106ce32b79c91ae3270	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/471db2c2d4f80ee94225a1ef246e4f5011733e50	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/aefd0a935625165a6ca36d0258d2d053901555df	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
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.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report