drm/amdgpu: add upper bound check on user inputs in signal ioctl

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-43400
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 15:16:51 UTC
Updated	2026-05-12 14:10:27 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: add upper bound check on user inputs in sig

Risk And Classification

EPSS: 0.000170000 probability, percentile 0.041320000 (date 2026-05-12)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected a292fdecd72834b3bec380baa5db1e69e7f70679 6fff5204d8aa26b1be50b6427f833bd3e8899c4f git
CNA	Linux	Linux	affected a292fdecd72834b3bec380baa5db1e69e7f70679 46630d966b99b0fc6cb01fef4110587f3375a0c0 git
CNA	Linux	Linux	affected a292fdecd72834b3bec380baa5db1e69e7f70679 ea78f8c68f4f6211c557df49174c54d167821962 git
CNA	Linux	Linux	affected 6.16
CNA	Linux	Linux	unaffected 6.16 semver
CNA	Linux	Linux	unaffected 6.18.19 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.9 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/46630d966b99b0fc6cb01fef4110587f3375a0c0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ea78f8c68f4f6211c557df49174c54d167821962	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/6fff5204d8aa26b1be50b6427f833bd3e8899c4f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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