drm/amd/display: Correct the defined value for AMDGPU_DMUB_NOTIFICATION_MAX

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

Summary

CVE	CVE-2024-46871
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-09 14:15:07 UTC
Updated	2026-05-05 15:14:56 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Correct the defined value for AMDGPU_

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

Problem Types: CWE-129

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability
High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 4562236b3bc0a28aeb6ee93b2d8a849a4c4e1c7c e1896f381d27466c26cb44b4450eae05cd59dfd0 gi
CNA	Linux	Linux	affected 4562236b3bc0a28aeb6ee93b2d8a849a4c4e1c7c 9f404b0bc2df3880758fb3c3bc7496f596f347d7 git
CNA	Linux	Linux	affected 4562236b3bc0a28aeb6ee93b2d8a849a4c4e1c7c 800a5ab673c4a61ca220cce177386723d91bdb37 g
CNA	Linux	Linux	affected 4562236b3bc0a28aeb6ee93b2d8a849a4c4e1c7c c592b6355b9b57b8e59fc5978ce1e14f64488a98 gi
CNA	Linux	Linux	affected 4562236b3bc0a28aeb6ee93b2d8a849a4c4e1c7c ad28d7c3d989fc5689581664653879d664da76f0 gi
CNA	Linux	Linux	affected 4.15
CNA	Linux	Linux	unaffected 4.15 semver
CNA	Linux	Linux	unaffected 5.15.174 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.109 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.50 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.9 6.10.* semver
CNA	Linux	Linux	unaffected 6.11 * original_commit_for_fix

References

Reference	Source	Link	Tag
git.kernel.org/stable/c/c592b6355b9b57b8e59fc5978ce1e14f64488a98	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/ad28d7c3d989fc5689581664653879d664da76f0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/e1896f381d27466c26cb44b4450eae05cd59dfd0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/9f404b0bc2df3880758fb3c3bc7496f596f347d7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/800a5ab673c4a61ca220cce177386723d91bdb37	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Mail
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

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