

CVE-2023-26083

Arm Mali GPU Kernel Driver Information Disclosure Vulnerability

CISA KEV since Apr 7, 2023

Actively exploited

Memory leak vulnerability in Mali GPU Kernel Driver in Midgard GPU Kernel Driver all versions from r6p0 - r32p0, Bifrost GPU Kernel Driver all versions from r0p0 - r42p0, Valhall GPU Kernel Driver all versions from r19p0 - r42p0, and Avalon GPU Kernel Driver all versions from r41p0 - r42p0 allows a non-privileged user to make valid GPU processing operations that expose sensitive kernel metadata.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 3.3 Low · NVD	EPSS 0.012 68.4th percentile · FIRST	CISA DEADLINE Apr 28, 2023 KEV since 2023 · 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	0.012 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 3.3	☐ 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
5th gen gpu architecture kernel driver	≥ r41p0 < r43p0	r43p0	NVD
bifrost gpu kernel driver	≥ r0p0 < r43p0	r43p0	NVD
midgard gpu kernel driver	≥ r6p0 ≤ r32p0	after r32p0	NVD
valhall gpu kernel driver	≥ r19p0 < r43p0	r43p0	NVD

Sources

Vendor guidance	developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities	NVD	nvd.nist.gov/vuln/detail/CVE-2023-26083
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-29957
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-26083		

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