



GPU DDK - UAF read of GLES3Context::psDrawParams and GLES3Context::psMode and UAF read/write of RMJob::apsCCBs

[MITRE](#)
[NVD](#)
[CVE.ORG](#)
[JSON API](#)
[Print: PDF](#)

Summary

CVE	CVE-2026-22165
State	PUBLISHED
Assigner	imaginationtech
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 16:16:29 UTC
Updated	2026-05-06 19:05:56 UTC
Description	A web page that contains unusual WebGPU content loaded into the GPU GLES render process and can trigger a write UAF

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from ADP

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

EPSS: 0.000130000 probability, percentile 0.022960000 (date 2026-05-05)

Problem Types: CWE-416 | CWE-416 CWE-416: Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unauthenticated

Unchanged

Confidentiality

None

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Imagination Technologies	Graphics DDK	affected 1.18 RTM custom	Linux, Android
CNA	Imagination Technologies	Graphics DDK	affected 23.2 RTM custom	Linux, Android
CNA	Imagination Technologies	Graphics DDK	affected 24.1 RTM 24.2 RTM custom	Linux, Android
CNA	Imagination Technologies	Graphics DDK	affected 25.1 RTM 25.3 RTM custom	Linux, Android
CNA	Imagination Technologies	Graphics DDK	unaffected 26.1 RTM custom	Linux, Android

References

Reference	Source	Link	Tags
www.imaginationtech.com/gpu-driver-vulnerabilities	367425dc-4d06-4041-9650-c2dc6aaa27ce	www.imaginationtech.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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