



# Arm Mali GPU Kernel Driver Use-After-Free Vulnerability

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

## Summary

<b>CVE</b>	CVE-2023-4211
<b>State</b>	PUBLIC
<b>Assigner</b>	arm-security@arm.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-10-01 18:15:00 UTC
<b>Updated</b>	2023-10-04 20:51:00 UTC
<b>Description</b>	A local non-privileged user can make improper GPU memory processing operations to gain access to already freed memor

## Risk And Classification

**EPSS:** 0.001970000 probability, percentile 0.416260000 (date 2026-04-01)

**CISA KEV:** Listed on 2023-10-03; due 2023-10-24; ransomware use Unknown

**Problem Types:** CWE-416

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Arm
<b>Product</b>	Mali GPU Kernel Driver
<b>Name</b>	Arm Mali GPU Kernel Driver Use-After-Free Vulnerability
<b>Required Action</b>	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
<b>Notes</b>	<a href="https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities">https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2023-4211">https://nvd.nist.gov/vuln/detail/CVE-2023-4211</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Arm</a>	<a href="#">5th Gen Gpu Architecture Kernel Driver</a>	All	All	All	All
Application	<a href="#">Arm</a>	<a href="#">Bifrost</a>	All	All	All	All
Application	<a href="#">Arm</a>	<a href="#">Midgard</a>	All	All	All	All
Application	<a href="#">Arm</a>	<a href="#">Valhall</a>	All	All	All	All

## References

References

Source

List

Reference	Source	Link
Vulnerable Arm GPU drivers under active exploitation. Patches may not be available   Ars Technica	MISC	<a href="https://arstechnica.com">arstechnica.com</a>
Chrome Releases: Long Term Support Channel Update for ChromeOS	MISC	<a href="https://chromereleases.googleblog.com">chromereleases.googleblog.com</a>
<a href="https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities">developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities</a>	MISC	<a href="https://developer.arm.com">developer.arm.com</a>
Chrome Releases: Stable Channel Update for ChromeOS / ChromeOS Flex	MISC	<a href="https://chromereleases.googleblog.com">chromereleases.googleblog.com</a>
Pixel Update Bulletin—September 2023   Android Open Source Project	MISC	<a href="https://source.android.com">source.android.com</a>
Arm warns of Mali GPU flaws likely exploited in targeted attacks	MISC	<a href="https://www.bleepingcomputer.com">www.bleepingcomputer.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [610513](#) Google Android Devices October 2023 Security Patch Missing
- [610516](#) Google Pixel Android September 2023 Security Patch Missing
- [610519](#) Google Android November 2023 Security Patch Missing for Samsung

© 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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)