

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## ARM's Zero-Day Flaw Leads to Improper GPU Memory Processing

Date of Publication

June 13, 2024

Admiralty Code

A1

TA Number

TA2024229

# Summary

**Discovered:** June 2024

**Affected Products:** Bifrost and Valhall GPU kernel drivers

**Impact:** Arm has issued a warning about a security vulnerability, CVE-2024-4610, which has been actively exploited in the wild. This memory-related vulnerability impacts the Bifrost and Valhall GPU kernel drivers. It allows a local non-privileged user to perform improper GPU memory processing operations, potentially granting access to already freed memory.

## 🔧 CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-4610	Arm Mali GPU Kernel Driver Use-After-Free Vulnerability	Bifrost and Valhall GPU kernel drivers	✓	✓	✓

# Vulnerability Details

## #1

Arm has addressed a memory-related vulnerability in Bifrost and Valhall GPU kernel drivers that is being actively exploited in the wild. The security issue tracked as CVE-2024-4610, is a use-after-free (UAF) vulnerability affecting all versions of Bifrost and Valhall drivers from r34p0 through r40p0.

## #2

Bifrost and Valhall GPU kernel drivers are integral components in software environments that power devices equipped with Arm GPUs based on the Bifrost and Valhall architectures. These GPUs are widely deployed in mobile devices and embedded systems and these drivers facilitate efficient operation of graphics and compute tasks.

## #3

This issue arises from a use-after-free error resulting from improper GPU memory processing operations. Essentially, a local non-privileged user can manipulate GPU memory operations inappropriately, potentially gaining access to memory that has already been freed.

## #4

Use-after-free (UAF) flaws occur when a program continues to reference a memory location after it has been freed. This flaw can lead to various security risks, including denial of service, information disclosure, and arbitrary code execution. Arm has addressed this issue in the latest version of the Bifrost and Valhall GPU Kernel Driver, r41p0. It is crucial for administrators to update their systems to this new version as soon as possible to protect against this vulnerability.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-4610	Bifrost GPU Kernel Driver: All versions from r34p0 to r40p0 Valhall GPU Kernel Driver: All versions from r34p0 to r40p0	cpe:2.3:a:arm:bifrost_gpu_kernel_driver:*:*:*:*:*:* cpe:2.3:a:arm:valhall_gpu_kernel_driver:*:*:*:*:*:*	CWE-416

## Recommendations



**Update:** To mitigate this risk, it is essential to update the Bifrost and Valhall GPU Kernel Driver to the latest version, r41p0.



**Vulnerability Management:** Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

# Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0002</u></b> Execution	<b><u>TA0040</u></b> Impact	<b><u>T1588</u></b> Obtain Capabilities
<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1499</u></b> Endpoint Denial of Service		

## Patch Details

It is important that you upgrade the Bifrost and Valhall GPU Kernel Drivers to the most recent version, r41p0, in order to mitigate this risk.

Links:

<https://developer.arm.com/downloads/-/mali-drivers/bifrost-kernel>

<https://developer.arm.com/downloads/-/mali-drivers/valhall-kernel>

## References

<https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**June 13, 2024 • 6:00 AM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)