**CVE-2023-6241** - A local non-privileged user can exploit a software **race condition** to perform **improper memory processing operations**. If the system’s memory is carefully prepared by the user, then this in turn causes a use-after-free.

* Gain arbitrary kernel code execution and root on the device

ARM Mali GPU:

* When using the Mali GPU driver, a user app first needs to create and initialize a kbase\_context kernel object (kbase\_context manages resources for each driver file opened)

The exploit targets the JIT (Just-In-Time) memory management in the Mali GPU, where a race condition allows for the unauthorized growth of a memory region during GPU fault handling. This discrepancy between the actual and intended memory sizes can lead to the GPU accessing freed memory pages. The exploit mechanism involves creating a JIT region, inducing a GPU fault to grow the region improperly, and then manipulating the size of this region to misalign the GPU's page table entries. This misalignment results in retained access to freed memory pages, which can be exploited to achieve kernel code execution by rewriting critical memory structures.

The exploit does not rely on dereferencing corrupted memory blocks or pointers, which MTE aims to prevent.