Un conjunto de cinco vulnerabilidades de seguridad de gravedad media en el controlador de GPU Mali de Arm, permanecieron sin parches en los dispositivos Android durante meses, a pesar de las correcciones publicadas por el fabricante de chips.

Google Project Zero, que describió e informó los errores, dijo que Arm solucionó las deficiencias en julio y agosto de 2022.

> *«Estas correcciones aún no han llegado a los dispositivos Android afectados (incluidos Pixel, Samsung, Xiaomi, Oppo y otros). Los dispositivos con una GPU Mali son actualmente vulnerables»,* dijo el investigador de Project Zero, Ian Beer.

Las vulnerabilidades, rastreadas de forma colectiva con los identificadores CVE-2022-33917 (putaje CVSS: 5.5) y CVE-2022-36449 (puntaje CVSS: 6.5), se refieren a un caso de procesamiento de memoria inadecuado, lo que permite que un usuario sin privilegios obtenga acceso a la memoria liberada.

La segunda vulnerabilidad, CVE-2022-36449, se puede armar aún más para escribir fuera de los límites del búfer y revelar detalles de las asignaciones de memoria, según un aviso emitido por Arm. La lista de controladores afectados se encuentra a continuación:

CVE-2022-33917

- Controlador de núcleo de GPU Valhall: Todas las versiones de r29p0-r38p0

CVE-2022-36449

- Midgard GPU Kernel Driver: Todas las versiones desde r4p0-r32p0
- Controlador Kernel GPU Bifrost: Todas las versiones desde r0p0-r38p0 y r39p0
- Controlador de núcleo de GPU Valhall: Todas las versiones de r19p0-r38p0 y r39p0

Los hallazgos destacan una vez más cómo las brechas de parches pueden hacer que millones de dispositivos sean vulnerables a la vez y ponerlos en riesgo de una mayor explotación por parte de los hackers.

> *«Así como se recomienda a los usuarios aplicar parches lo más rápido posible una vez que esté disponible una versión que contenga actualizaciones de seguridad, lo mismo se aplica a los proveedores y empresas»,* dijo Beer.

> *«Las empresas deben permanecer atentas, seguir de cerca las fuentes ascendentes y hacer todo lo posible para proporcionar parches completos a los usuarios lo antes posible».*