Imagination GPU Driver Vulnerabilities

View our Product Security Policy

This page contains summary details of security vulnerabilities reported on Imagination Technologies graphics drivers.

August 2023

Title	GPU – PMRWritePMPageList write OOB due to integer overflow
Our Reference	A-278926273
CVE Reference	CVE-2023-21217
Date Posted	28th June 2024
Versions affected	DDK Releases up to and including 23.1
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger OOB write to kernel heap memory.

Resolution	The DDK kernel module has been updated to address this issue in these GPU system calls.

Title	GPU – UAF in PMR_ReadBytes when destroying FreeList
Our Reference	A-278927832
CVE Reference	CVE-2023-21163
Date Posted	28th June 2024
Versions affected	DDK Releases up to and including 23.1
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free exceptions in the kernel module.
Resolution	The DDK kernel module has been updated to address this issue in the affected GPU system calls.

Title	GPU – UAF in RGXUnbackingZSBuffer
Our Reference	A-278927608
CVE Reference	CVE-2023-21162
Date Posted	28th June 2024
Versions affected	DDK Releases up to and including 23.1
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free exceptions in the kernel module.
Resolution	The DDK kernel module has been updated to address this issue in the affected GPU system calls.

Title	GPU – Object psReservation UAF in RGXBackingZSBuffer when invoking PVRSRVBridgeRGXPopulateZSBuffer
Our Reference	A-278929010
CVE Reference	CVE-2023-21166
Date Posted	28th June 2024
Versions affected	DDK Releases up to and including 23.1
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU

	system calls to trigger use-after-free exceptions in the kernel module.
Resolution	The DDK kernel module has been updated to address this issue in the affected GPU system calls.

Title	GPU – UAF in DevmemIntMapPMR when invoking PVRSRVBridgeRGXPopulateZSBuffer
Our Reference	A-278928734
CVE Reference	CVE-2023-21164
Date Posted	28th June 2024
Versions affected	DDK Releases up to and including 23.1
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free exceptions in the kernel module.
Resolution	The DDK kernel module has been updated to address this issue in the affected GPU system calls.

September 2023

Title	GPU – GPU OOB access to physical memory from mis-configured heap
Our Reference	PP-137204-X.2
CVE Reference	None
Date Posted	19th September 2023
Versions affected	DDK Releases up to and including 1.19
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access out of bounds memory
Resolution	The DDK kernel module has been updated to introduce protection to prevent misuse of heaps

Title	GPU – GPU OOB access to physical memory from mis-configured heap
Our Reference	PP-137205-X.3
CVE Reference	None
Date Posted	19th September 2023

Versions affected	DDK Releases up to and including 1.19
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access out of bounds memory
Resolution	The DDK kernel module has been updated to introduce protection to prevent misuse of heaps

Title	GPU – OOB access to kernel memory when creating a graphics buffer
Our Reference	PP-137207-X.5
CVE Reference	None
Date Posted	19th September 2023
Versions affected	DDK Releases 1.15 and later, up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access out of bounds kernel memory
Resolution	The DDK kernel module has been updated to introduce protection to prevent misuse when creating graphics buffers

Title	GPU – Access to GPU buffer memory after it has been freed
Our Reference	PP-137212-X.7
CVE Reference	None
Date Posted	19th September 2023
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access freed memory
Resolution	The DDK kernel module has been updated to ensure some GPU buffer memory will not be reused after it is freed

Title	GPU – R/W Arbitrary physical pages with PFNs from uninitialized stack variables
Reference	A-288116176
CVE Reference	CVE-2023-21263
Date Posted	6th June 2024

Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write parts of physical memory from user-space
Resolution	The DDK kernel module has been updated to introduce protection to prevent this unauthorised access to memory

Title	GPU – Write OOB in DevmemIntChangeSparse due to integer overflow
Reference	A-288117034
CVE Reference	CVE-2023-21401
Date Posted	6th June 2024
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access OOB kernel memory
Resolution	The DDK kernel module has been updated to introduce protection to reject incorrect user-mode parameters given to this GPU system call

Title	GPU – mmap unexpected physical addresses due to OOB read in _PMRLogicalOffsetToPhysicalOffset
Reference	A-289053114
CVE Reference	CVE-2023-35688
Date Posted	6th June 2024
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access OOB kernel memory
Resolution	The DDK kernel module has been updated to introduce protection to reject incorrect user-mode parameters given to this GPU system call

Title	GPU – UAF in RGXDestroyHWRTData due to firmware response timeout
Reference	A-288114043
CVE Reference	CVE-2023-35690

Date Posted	6th June 2024
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free kernel exceptions
Resolution	The DDK kernel module has been updated to address this issue in this GPU system call

Title	GPU – UAF in RGXDestroyZSBufferKM due to firmware response timeout
Reference	A-288112355
CVE Reference	CVE-2023-21403
Date Posted	6th June 2024
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free kernel exceptions
Resolution	The DDK kernel module has been updated to address this issue in this GPU system call

Title	GPU – Read OOB in _MMU_GetPTInfo due to invalid page size
Reference	A-288115093
CVE Reference	CVE-2023-21402
Date Posted	6th June 2024
Versions affected	DDK Releases up to and including 1.19
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to read OOB kernel memory
Resolution	The DDK kernel module has been updated to introduce protection to reject incorrect user-mode parameters given to th GPU system call affected

October 2023

Title	GPU – GPU can R/W arbitrary freed physical pages due to PMR object reference count mismanagement in DevmemIntMapPages

Our References	PP-137206-X.4 PP-137216-X.11
CVE Reference	CVE-2023-35685
Date Posted	2nd October 2023
Versions affected	DDK Releases up to and including 1.18
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access freed memory from the GPU.
Resolution	The DDK kernel module has been updated to correct reference counting for these objects to prevent the issue.

Title	GPU – GPU OOB access to physical memory from mis-configured reservation
Our Reference	PP-137214-X.1
CVE Reference	None
Date Posted	2nd October 2023
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access OOB memory from the GPU.
Resolution	The DDK kernel module has been updated to introduce protection to reject incorrect user-mode parameters given to GPU system calls.

Title	GPU – Driver can leak kernel information through IOCTL calls
Our Reference	PP-137214-X.9
CVE Reference	None
Date Posted	2nd October 2023
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger a leak of kernel data or trigger a kernel exception.
Resolution	The DDK kernel module has been updated to introduce protection to prevent misuse of the IOCTL interface.

Title	GPU – Reservation object UAF in DevmemIntUnmapPMR

Our References	PP-137217-X.12 PP-137443-X.22
CVE Reference	CVE-2023-21165
Date Posted	12th October 2023
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger a UAF kernel exception.
Resolution	The DDK kernel module has been updated to introduce protection to prevent this use-after-free issue.

Title	GPU Driver can leak kernel information via device memory history IOCTL calls
Reference	A-289116037
CVE Reference	None
Date Posted	20th May 2024
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to leak data from uninitialised kernel heap memory.
Resolution	The DDK kernel module has been updated to introduce protection to prevent misuse of this IOCTL interface.

Title	GPU – UAF during DIContext/HWRTDAtaSet resource clean-up when OSCopyToUser fails
References	C-290879631 C-290921312
CVE Reference	None
Date Posted	20th May 2024
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free kernel exceptions.
Resolution	The DDK kernel module has been updated to introduce protection to prevent this use-after-free.

November 2023

Title	GPU can read and write freed physical memory pages of sparse allocations
Reference	None
CVE Reference(s)	CVE-2023-35686 CVE-2023-35659
Date Posted	13th May 2024
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to read and write freed physical memory from the GPU.
Resolution	The DDK kernel module has been updated to introduce protection to prevent improper use of GPU system calls.

Title	GPU – User-space can read & write arbitrary freed memory with DevmemIntChangeSparse remap mode
Reference	C-299853339
CVE Reference	None
Date Posted	13th May 2024
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to read and write arbitrary freed physical memory from user-space.
Resolution	The DDK kernel module has been updated to introduce protection to prevent improper use of GPU system calls.

Title	GPU – OOB Write In PhysmemCreateNewDmaBufBackedPMR
Reference	C-292164683
CVE Reference	None
Date Posted	13th May 2024
Versions affected	DDK Releases up to and including 23.2

Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access OOB kernel memory.
Resolution	The DDK kernel module has been updated to introduce protection to reject incorrect user-mode parameters given to GPU system calls.

Title	GPU – Shader shared memory can be tampered with by the GPU
Reference	A-300484838
CVE Reference	CVE-2024-23714
Date Posted	13th May 2024
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access and/or corrupt shared driver memory using the GPU.
Resolution	The DDK kernel module has been updated to introduce protection to prevent improper use of the GPU system calls.

December 2023

Title	GPU can read and write arbitrary physical memory pages
Reference	A-299923390
CVE Reference	CVE-2024-23715
Date Posted	22nd March 2024
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to read and write arbitrary physical memory from the GPU.
Resolution	The DDK kernel module has been updated to introduce protection to prevent improper use of GPU system calls.

Title	GPU – Driver controllable OOB writes due to integer overflow in DevmemIntChangeSparse
Reference	C-299384059
CVE Reference	None

Date Posted	22nd March 2024
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access OOB kernel memory.
Resolution	The DDK kernel module has been updated to introduce protection to reject incorrect user-mode parameters given to GPU system calls.

Title	GPU – User-space can read & write arbitrary freed memory with DevmemIntChangeSparse race condition
Reference	C-299447904
CVE Reference	None
Date Posted	22nd March 2024
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to read and write arbitrary freed physical memory from user-space.
Resolution	The DDK kernel module has been updated to introduce protection to prevent improper use of GPU system calls.

January 2024

Title	GPU – Leftover locals – local memory data leak
Reference	None
CVE Reference	CVE-2023-4969
Date Posted	16th January 2024
Versions affected	DDK Releases up to and including 23.2
Vulnerability	Software installed and run as a non-privileged user may execute improper GPU compute kernels to leak uninitialised local data from the GPUs internal local memory.
Resolution	The user-mode drivers and firmware have been updated to introduce protection to prevent this misuse of local memory.

February 2024

Title	GPU – Re-use of MMU PT memory can allow GPU shader to R/W OOB to freed memory in rare situations
Our Reference	PP-137442-X.21
CVE Reference	None
Originator Reference	None
Date Posted	22nd February 2024
Versions affected	DDK Releases up to and including 23.3
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write freed physical memory from the GPU.
Resolution	The DDK kernel module has been updated to prevent situations from arising where this vulnerability is present.

Title	GPU can read and write freed physical memory pages after a virtual range is destroyed
Our Reference	PP-148694
CVE Reference	CVE-2024-23711
Originator Reference	None
Date Posted	22nd February 2024
Versions affected	DDK Releases up to and including 23.3
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write freed physical memory from the GPU.
Resolution	The DDK kernel module has been updated to ensure GPU virtual mappings are removed when a virtual range is destroyed.

Title	GPU – Uninitialised physical memory causes arbitrary content leak to user-mode on UMA systems
Our Reference	PP-159144
CVE Reference	None

Originator Reference	C-305594806
Date Posted	22nd February 2024
Versions affected	DDK Releases up to and including 23.3
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read kernel and other sensitive information from GPU buffers.
Resolution	The DDK kernel module has been updated to ensure the previous content of memory pages used in GPU buffers are cleared before re-using them in a different context.

March 2024

Title	GPU – RA_FreeMultiSparse OOBs access can trigger UAF of LMA physical memory page
Our Reference	PP-158856
CVE Reference	None
Originator Reference	None
Date Posted	8th March 2024
Versions affected	DDK Releases up to and including 23.2 RTM1
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write freed physical memory in VRAM from the GPU.
Resolution	The DDK kernel module has been updated to prevent the OOB issue so that the UAF can no longer occur.

Title	GPU – UAF race condition between DevmemIntPFNotify and DevmemIntCtxRelease
Our Reference	PP-159077
CVE Reference	CVE-2024-23716
Originator Reference	A-300480809
Date Posted	22nd March 2024

Versions affected	DDK Releases up to and including 23.3
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free kernel exceptions.
Resolution	The DDK kernel module has been updated to introduce protection to prevent this use-after-free issue.

Title	GPU – Exhaustion of memory in DevmemIntHeapCreate triggers system OOM
Our Reference	PP-159018
CVE Reference	None
Originator Reference	C-316857793
Date Posted	22nd March 2024
Versions affected	DDK Releases up to and including 23.3
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to exhaust available system memory leading to instability.
Resolution	The DDK kernel module has been updated to introduce protection to prevent improper use of GPU system calls.

Title	GPU – UAF caused in RGXCreateZSBufferKM due to improper error handling code
Our Reference	PP-159039
CVE Reference	CVE-2024-23696
Originator Reference	A-320199249, PP-159059
Date Posted	25th March 2024
Versions affected	DDK Releases up to and including 23.3
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free kernel exceptions.
Resolution	The DDK kernel module has been updated to introduce protection to prevent improper use of GPU system calls.

April 2024

Title	GPU – PowerVR: DevmemIntUnexportCtx destroys export before unlinking it, leading to UAF
Our Reference	PP-159069
CVE Reference	CVE-2024-34725
Originator Reference	None
Date Posted	5th April 2024
Versions affected	DDK Releases up to and including 23.3
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free kernel exceptions.
Resolution	The DDK kernel module has been updated to address this improper use of GPU system calls.

Title	GPU – _MapPhysicalSparseAlloc issue leads to OOB write to VRAM memory page
Our Reference	PP-159017
CVE Reference	None
Originator Reference	None
Date Posted	5th April 2024
Versions affected	DDK Releases up to and including 23.3
Vulnerability	The kernel module can in some rare scenarios write overflow (OOB) GPU memory buffers which leads to graphics memory corruption.
Resolution	The DDK kernel module has been updated to correct this issue seen on systems with dedicated graphics memory (VRAM).

Title	GPU – Kernel heap OOB write in RGXFWChangeOSidPriority
Our Reference	PP-159016
CVE Reference	CVE-2024-23698
Originator Reference	A-320199679

Date Posted	15th April 2024
Versions affected	DDK Releases up to and including 23.3
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access OOB kernel memory.
Resolution	The DDK kernel module has been updated to introduce protection to reject incorrect user-mode parameters given to this GPU system call.

Title	GPU – UAF caused in RGXCreateHWRTData_aux due to improper error handling code
Our Reference	PP-159040
CVE Reference	CVE-2024-23697
Originator Reference	A-320199241
Date Posted	15th April 2024
Versions affected	DDK Releases up to and including 23.3
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free kernel exceptions.
Resolution	The DDK kernel module has been updated to address this improper use of GPU system calls.

Title	GPU – Linux driver shared data and shader programs can be corrupted from user-mode code
Our Reference	PP-159075
CVE Reference	CVE-2024-34726
Originator Reference	None
Date Posted	19th April 2024
Versions affected	DDK Releases up to and including 23.3
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to corrupt shared graphics buffers providing common data and shaders.
Resolution	The DDK kernel module has been updated to introduce protection to prevent improper use of GPU system calls.

Title	GPU – Kernel heap OOB write in CacheOpPMRExec due to integer overflow
Our Reference	PP-159082
CVE Reference	CVE-2024-23695
Originator Reference	A-326167784
Date Posted	19th April 2024
Versions affected	DDK Releases up to and including 23.3
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access OOB kernel memory.
Resolution	The DDK kernel module has been updated to introduce protection to reject incorrect user-mode parameters given to this GPU system call.

Title	GPU – OSAtomicAddUnless() returns wrong results affecting the fix for CVE-2021-0951
Our Reference	PP-159098
CVE Reference	None
Originator Reference	None
Date Posted	19th April 2024
Versions affected	DDK Releases up to and including 23.3
Vulnerability	This issue covers a functional deficiency in the implementation and use of OSAtomicAddUnless on non-Linux based operating systems.
Resolution	The DDK kernel module has been updated to correct the implementation of OSAtomicAddUnless function.

May 2024

Title	GPU – Overflow of refcount in _MMU_AllocLevel leads to arbitrary read and write of physical memory
Our Reference	PP-159087
CVE Reference	CVE-2024-31333

Originator Reference	C-324910147
Date Posted	17th May 2024
Versions affected	DDK Releases up to and including 24.1
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write arbitrary physical memory from the GPU.
Resolution	The DDK kernel module has been updated to introduce protection to prevent improper use of GPU system calls that lead to this issue.

Title	GPU – Use-after-free read in _UnrefAndMaybeDestroy
Our Reference	PP-159089
CVE Reference	CVE-2024-34724
Originator Reference	None
Date Posted	17th May 2024
Versions affected	DDK Releases up to and including 1.19
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free kernel exceptions.
Resolution	The DDK kernel module has been updated to introduce protection to prevent this use-after-free issue.

Title	GPU – DevmemIntChangeSparse issue can briefly allow read and write to freed physical memory pages
Our Reference	PP-159372
CVE Reference	CVE-2024-31335
Originator Reference	None
Date Posted	17th May 2024
Versions affected	DDK Releases up to and including 24.1
Vulnerability	Software installed and run as a non-privileged user may exploit a small window of opportunity to access freed memory.

Resolution	The DDK kernel module has been updated to address the code issue that allows this exploit.

Title	GPU – Inconsistent parameters to PhysmemNewRamBackedPMR leaks memory pages
Our Reference	PP-159422
CVE Reference	None
Originator Reference	None
Date Posted	31st May 2024
Versions affected	DDK Releases up to and including 24.1
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to exhaust available graphics memory leading to instability.
Resolution	The DDK kernel module has been updated to introduce protection to prevent improper use of GPU system calls.

Title	GPU – PowerVR: Wrong order of operations in DevmemIntUnmapPMR2 may lead to temporarily dangling PTEs
Our Reference	PP-159433
CVE Reference	CVE-2024-31335
Originator Reference	None
Date Posted	31st May 2024
Versions affected	DDK Releases up to and including 24.1
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free kernel exceptions.
Resolution	The DDK kernel module has been updated to address the code issue that allows this exploit.

Title	GPU – PowerVR: DevmemXIntMapPages allows mapping sDevZeroPage and sDummyPage without holding reference
Our Reference	PP-159437
CVE Reference	CVE-2024-31334

Originator Reference	None
Date Posted	31st May 2024
Versions affected	DDK Releases up to and including 24.1
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free kernel exceptions.
Resolution	The DDK kernel module has been updated to address the code issue that allows this exploit.

June 2024

Title	GPU – PowerVR: out-of-bounds write of firmware addresses in PVRSRVRGXKickTA3DKM
Our Reference	PP-159407
CVE Reference	CVE-2024-31336
Originator Reference	None
Date Posted	14th June 2024
Versions affected	DDK Releases up to and including 24.1
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access OOB kernel memory.
Resolution	The DDK kernel module has been updated to introduce protection to reject incorrect user-mode parameters given to this GPU system call.

Title	GPU – PowerVR: Uninitialized memory disclosure (and crash due to OOB reads) in hwperf_host stream
Our Reference	PP-159186
CVE Reference	None
Originator Reference	None
Date Posted	14th June 2024
Versions affected	DDK Releases up to and including 24.1

Vulnerability	Under certain circumstances the driver could return a limited amount of uninitialised kernel stack memory to user-space.
Resolution	The DDK kernel module has been updated to ensure kernel stack data in this instance is not returned to user-space.

Title	GPU – PowerVR: Driver doesn’t sanitize ZS-Buffer / MSAA scratch firmware addresses
Our Reference	PP-159408
CVE Reference	CVE-2024-31337
Originator Reference	None
Date Posted	28th June 2024
Versions affected	DDK Releases up to and including 24.1
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to access OOB firmware memory.
Resolution	The DDK kernel module has been updated to introduce protection to prevent firmware memory access in this way.

July 2024

Title	GPU – Multiple sparse mappings in DevmemIntChangeSparse2 leads to UAF of physical memory from GPU
Our Reference	PP-159339
CVE Reference	CVE-2024-34729
Originator Reference	None
Date Posted	8th July 2024
Versions affected	DDK Releases up to and including 24.1
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write freed physical memory from the GPU.
Resolution	The DDK kernel module has been updated to address this improper use of GPU system calls.

Title	GPU – In-flight GPU shader or kernel can read and write to buffer pages after the PMR has been freed
Our Reference	PP-159752
CVE Reference	CVE-2024-40649
Originator Reference	None
Date Posted	26th July 2024
Versions affected	DDK Releases up to and including 24.1
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write freed physical memory from the GPU.
Resolution	The DDK kernel module has been updated to introduce protection to address the race-condition vulnerability that was exploited in this particular attack.

Title	GPU – PowerVR: integer overflows in DevmemXIntMapPages and DevmemXIntUnmapPages, exploitable as dangling GPU PTEs
Our Reference	PP-159653
CVE Reference	CVE-2024-34733
Originator Reference	None
Date Posted	26th July 2024
Versions affected	DDK Releases up to and including 24.1
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write freed physical memory from the GPU.
Resolution	The DDK kernel module has been updated to address this improper use of GPU system calls.

Title	GPU – PowerVR: wrapping addition in _DevmemXReservationPageAddress causes MMU operation at wrong address
Our Reference	PP-159654
CVE Reference	CVE-2024-34748
Originator Reference	None
Date Posted	26th July 2024

Versions affected	DDK Releases up to and including 24.1
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write freed physical memory from the GPU.
Resolution	The DDK kernel module has been updated to address this improper use of GPU system calls.

Title	GPU – In-flight GPU shader or kernel can read/write to freed buffer pages in DevmemIntChangeSparse2
Our Reference	PP-159753
CVE Reference	CVE-2024-40651
Originator Reference	None
Date Posted	26th July 2024
Versions affected	DDK Releases up to and including 24.1
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write freed physical memory from the GPU.
Resolution	The DDK kernel module has been updated to introduce protection to address the race-condition vulnerability that was exploited in this particular attack.

Title	GPU – PowerVR: On-demand PMR physical memory is freed before GPU TLB invalidation
Our Reference	PP-159595
CVE Reference	CVE-2024-34732
Originator Reference	None
Date Posted	26th July 2024
Versions affected	DDK Releases up to and including 24.1
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write freed physical memory from the GPU.
Resolution	The DDK kernel module has been updated to introduce protection to address the race-condition vulnerability that was exploited in this particular attack.

August 2024

Title	GPU – PowerVR: Weaknesses identified in the deferred PMR free TLB invalidation security fix
Our Reference	PP-160180
CVE Reference	CVE-2024-40670
Originator Reference	None
Date Posted	15th August 2024
Versions affected	DDK Releases up to and including 24.2
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write freed physical memory from the GPU.
Resolution	The DDK kernel module has been updated to introduce protection to address the race-condition weaknesses that can be exploited in this particular attack.

Title	GPU – PowerVR: TLB Invalidate UAF of physical pages in sparse and on-demand PMRs on LMA systems (DDK 1.17 and earlier)
Our Reference	PP-160206
CVE Reference	CVE-2024-40669
Originator Reference	None
Date Posted	15th August 2024
Versions affected	DDK Releases up to and including 1.17
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write freed physical memory from the GPU.
Resolution	The DDK kernel module has been updated to introduce protection to address the race-condition vulnerability that was exploited in this particular attack.

Title	GPU DDK – DevmemIntChangeSparse2 UAF on PMRGetUID call
Our Reference	PP-160094
CVE Reference	CVE-2024-40671
Originator Reference	None

Date Posted	23rd August 2024
Versions affected	DDK Releases up to and including 24.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free kernel exceptions.
Resolution	The DDK kernel module has been updated to address this improper use of GPU system calls.

September 2024

Title	GPU – PowerVR: DEVMEMXINT_RESERVATION::ppsPMR references PMRs but does not lock their physical addresses
Our Reference	PP-159931
CVE Reference	CVE-2024-34747
Originator Reference	None
Date Posted	6th September 2024
Versions affected	DDK Releases up to and including 24.1
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write freed physical memory from the GPU.
Resolution	The DDK kernel module has been updated to address this improper use of GPU system calls.

Title	GPU – Incomplete check of the PMMETA_PROTECT flag in PowerVR driver leads to arbitrary kernel physical page write
Our Reference	PP-160287
CVE Reference	CVE-2024-43077
Originator Reference	C-349746415
Date Posted	20th September 2024
Versions affected	DDK Releases up to and including 24.2
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to write arbitrary physical memory from the GPU.

Resolution	The DDK kernel module has been updated to introduce protection to prevent improper use of GPU system calls.

October 2024

Title	GPU DDK – PowerVR: TLB invalidate UAF of dma_buf imported into multiple GPU devices
Our Reference	PP-160192
CVE Reference	CVE-2024-43701
Originator Reference	None
Date Posted	4th October 2024
Versions affected	DDK Releases up to and including 24.2 RTM1
Vulnerability	Software installed and run as a non-privileged user may conduct GPU system calls to read and write freed physical memory from the GPU.
Resolution	The DDK kernel module has been updated to introduce protection to prevent improper use of GPU system calls.

November 2024

Title	GPU DDK – PowerVR: PVRSRVAcquireProcessHandleBase can cause psProcessHandleBase reuse when PIDs are reused
Our Reference	PP-160496
CVE Reference	CVE-2024-43704
Originator Reference	None
Date Posted	15th November 2024
Versions affected	DDK Releases up to and including 24.2 RTM1
Vulnerability	Software installed and run as a non-privileged user may conduct improper GPU system calls to gain access to the graphics buffers of a parent process.
Resolution	The DDK kernel module has been updated to prevent the situation that allows this issue to occur.

If you have any questions on these vulnerabilities, please reach out to your Imagination Technologies support representative.

Technology

GPU (Graphics Processing Unit)

AI & Compute

Ray Tracing

Functional Safety

Software Solutions

Open Access

Design Optimisation Kit

Product Finder

Developers

Developers

PowerVR SDK and Tools

Developer Downloads

Developer Documentation

Developer Support

Developer Forums

GPU Driver Vulnerabilities

About Imagination

About Us

Career Opportunities

Imagining a Sustainable Future

Corporate Social Responsibility

Imagination Leadership

Imagination Partners

Contact Imagination

Stay Connected

Sign up to receive the latest news and product updates from Imagination straight to your inbox.

Subscribe

Applications

Automotive

Consumer Electronics

Desktop

Mobile

News & Insights

News

Resources

Blog

Events

Webinars

Imagination Glossary

The Future of Automotive

Our Policies

Privacy Policy

Use of Cookies

Terms of Use

Trademarks

Quality Policy

Product Security Policy

Modern Slavery Act