

# GPU DRIVER VULNERABILITIES

[View our Product Security Policy](#)

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

2026

2024

2025

We use cookies to improve your experience and to measure the performance of our website content. You can either consent to accept all the cookies or choose which ones you want.

[Change settings](#)

[Accept All](#)

## January 2026

<b>Title</b>	GPU DDK – GPU Register value contents leaked fr
<b>Our Reference</b>	PSP-19
<b>CVE Reference</b>	CVE-2025- 25176
<b>Originator Reference</b>	PP-171174
<b>Date Posted</b>	9th January 2026
<b>Versions affected</b>	DDK Releases up to and including 25.2 RTM
<b>Vulnerability</b>	Intermediate register values of secure workloads c non-secure environment of a platform.
<b>Resolution</b>	The DDK has been updated to introduce protectio

<b>Title</b>	GPU DDK – Reservation::psMappedPMR can chan
<b>Our Reference</b>	PSP-225
<b>CVE Reference</b>	CVE-2025-58411
<b>Originator Reference</b>	PP-173070
<b>Date Posted</b>	9th January 2026
<b>Versions affected</b>	DDK Releases up to and including 25.2 RTM
<b>Vulnerability</b>	Software installed and run as a non-privileged use resources reference counting creating a write use
<b>Resolution</b>	The DDK kernel module has been updated to addr prematurely free whilst references exist.

<b>Title</b>	GPU DDK –
<b>Our Reference</b>	PSP-226
<b>CVE Reference</b>	CVE-2025-
<b>Originator Reference</b>	PP-173069
<b>Date Posted</b>	9th January
<b>Versions affected</b>	DDK Releas

We use cookies to improve your experience and to measure the performance of our website content. You can either consent to accept all the cookies or choose which ones you want.

Change settings

Accept All

<b>Vulnerability</b>	Software installed and run as a non-privileged use reference counting creating a potential use after fi
<b>Resolution</b>	The DDK kernel module has been updated to addr prematurely free whilst references exist.

<b>Title</b>	GPU DDK – PVRSRVBridgeHeapCfgHeap(ConfigN
<b>Our Reference</b>	PSP-242
<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-173163
<b>Date Posted</b>	9th January 2026
<b>Versions affected</b>	DDK Releases up to and including 25.2 RTM
<b>Vulnerability</b>	Software installed and run as a non-privileged use kernel heap memory.
<b>Resolution</b>	The DDK kernel module has been updated to intro

<b>Title</b>	GPU DDK – Disguised freelist buffers passed to RC corrupting memory
<b>Our Reference</b>	PSP-203
<b>CVE Reference</b>	CVE-2025-58409
<b>Originator Reference</b>	None
<b>Date Posted</b>	12th Jan 2026
<b>Versions affected</b>	DDK Releases up to and including 25.2 RTM
<b>Vulnerability</b>	Software installed and run as a non-privileged use arbitrary physical memory pages.  Under certa pages in us
<b>Resolution</b>	The DDK ke to arbitrary

<b>Title</b>	GPU DDK –
<b>Our Reference</b>	PSP-222
<b>CVE Reference</b>	CVE-2025-

We use cookies to improve your experience and to measure the performance of our website content. You can either consent to accept all the cookies or choose which ones you want.

Change settings

Accept All

<b>Originator Reference</b>	PVR-LSBD-2025-222
<b>Date Posted</b>	23rd Jan 2026
<b>Versions affected</b>	DDK Releases up to and including 25.2 RTM
<b>Vulnerability</b>	A web page that contains unusual GPU shader code free crash in the GPU shader compiler library. On c could enable further exploits on the device.
<b>Resolution</b>	The DDK compiler library has been updated to har process executing the shader compilation.

## February 2026

<b>Title</b>	GPU DDK – libufwriter read UAF at llvm::MetadataT
<b>Our Reference</b>	PSP-264
<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-172923
<b>Date Posted</b>	20th February 2026
<b>Versions affected</b>	DDK Releases starting from 24.2 RTM1 up to and i
<b>Vulnerability</b>	A web page that contains unusual GPU shader code free crash in the GPU shader compiler library. On c could enable further exploits on the device.
<b>Resolution</b>	The DDK compiler library has been updated to har process executing the shader compilation.

<b>Title</b>	GPU DDK – libusc NPD at MarkGradient_MarkArg c
<b>Our Reference</b>	PSP-262
<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-173017
<b>Date Posted</b>	20th Febru
<b>Versions affected</b>	DDK Releas
<b>Vulnerability</b>	A web page dereferenc this could e

We use cookies to improve your experience and to measure the performance of our website content. You can either consent to accept all the cookies or choose which ones you want.

Change settings

Accept All

<b>Resolution</b>	The DDK compiler library has been updated to handle process executing the shader compilation.
-------------------	---

## March 2026

<b>Title</b>	GPU DDK – Insufficient permission check in Physr
<b>Our Reference</b>	PSP-251
<b>CVE Reference</b>	CVE-2026-21736
<b>Originator Reference</b>	PP-171245
<b>Date Posted</b>	9th March 2026
<b>Versions affected</b>	DDK Releases up to and including 25.1 RTM2
<b>Vulnerability</b>	Software installed and run as a non-privileged user only wrapped user-mode memory and files.
<b>Resolution</b>	The DDK kernel module has been updated to address mode memory from being exported with incompat

<b>Title</b>	GPU DDK – Freelist PFN leak via mprotect
<b>Our Reference</b>	PSP-290
<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-173475
<b>Date Posted</b>	9th March 2026
<b>Versions affected</b>	DDK Releases up to and including 25.3 RTM
<b>Vulnerability</b>	Software installed and run as a non-privileged user physical address
<b>Resolution</b>	The DDK kernel

<b>Title</b>	GPU DDK –
<b>Our Reference</b>	PSP-263
<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-172824
<b>Date Posted</b>	9th March 2026

We use cookies to improve your experience and to measure the performance of our website content. You can either consent to accept all the cookies or choose which ones you want.

Change settings

Accept All

<b>Versions affected</b>	DDK Releases up to and including 25.3 RTM
<b>Vulnerability</b>	A web page that contains unusual GPU shader code dereference crash in the GPU shader compiler library. This could enable for example further denial of service.
<b>Resolution</b>	The DDK compiler library has been updated to handle the process executing the shader compilation.

<b>Title</b>	GPU DDK – libufwriter OOB read at (llvm::APIInt::compile)
<b>Our Reference</b>	PSP-265
<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-172817
<b>Date Posted</b>	9th March 2026
<b>Versions affected</b>	DDK Releases up to and including 25.2 RTM
<b>Vulnerability</b>	A web page that contains unusual GPU shader code OOB read in the GPU shader compiler library. On certain devices this could lead to crashes or enable further exploits on the device.
<b>Resolution</b>	The DDK compiler library has been updated to handle the process executing the shader compilation.

<b>Title</b>	GPU DDK – libusc OOB write at ConvertSwitchToA
<b>Our Reference</b>	PSP-223
<b>CVE Reference</b>	CVE-2026-21732
<b>Originator Reference</b>	PVR-LSBD-2025-223
<b>Date Posted</b>	20th March 2026
<b>Versions affected</b>	DDK Releases up to and including 25.2 RTM
<b>Vulnerability</b>	A web page that contains unusual GPU shader code OOB write crash in the GPU shader compiler library. This could enable for example further denial of service.
<b>Resolution</b>	The DDK compiler library has been updated to handle the process executing the shader compilation.

<b>Title</b>	GPU DDK –
--------------	-----------

We use cookies to improve your experience and to measure the performance of our website content. You can either consent to accept all the cookies or choose which ones you want.

Change settings

Accept All

<b>Our Reference</b>	PSP-257
<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-173312
<b>Date Posted</b>	20th March 2026
<b>Versions affected</b>	DDK Releases starting from 25.1 RTM1 up to and i
<b>Vulnerability</b>	Software installed and run as a non-privileged use resources reference counting creating a read use
<b>Resolution</b>	The DDK kernel module has been updated to addr prematurely free whilst references exist.

<b>Title</b>	GPU DDK – libufwriter NPD at CSE_InstCmpCB du
<b>Our Reference</b>	PSP-274
<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-172873
<b>Date Posted</b>	20th March 2026
<b>Versions affected</b>	DDK Releases starting from 25.1 RTM2 up to and i
<b>Vulnerability</b>	A web page that contains unusual GPU shader code dereference crash in the GPU shader compiler libr this could enable for example further denial of ser
<b>Resolution</b>	The DDK compiler library has been updated to har process executing the shader compilation.

<b>Title</b>	GPU DDK – Unsafe writing of MMU PT entries on s
<b>Our Reference</b>	PSP-289
<b>CVE Reference</b>	CVE-2026-
<b>Originator Reference</b>	None
<b>Date Posted</b>	20th March
<b>Versions affected</b>	DDK Releas
<b>Vulnerability</b>	Software in accidental v
<b>Resolution</b>	The DDK ke

We use cookies to improve your experience and to measure the performance of our website content. You can either consent to accept all the cookies or choose which ones you want.

Change settings

Accept All

<b>Title</b>	GPU DDK – Freelist PFN leak via ptrace
<b>Our Reference</b>	PSP-291
<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-173476
<b>Date Posted</b>	20th March 2026
<b>Versions affected</b>	DDK Releases up to and including REL/25.3 RTM
<b>Vulnerability</b>	Software installed and run as a non-privileged user can leak physical addresses.
<b>Resolution</b>	The DDK kernel module has been updated to address the issue.

## April 2026

<b>Title</b>	GPU DDK – libusc Stack overflow at DrawArrays and DrawArraysInstanced
<b>Our Reference</b>	PSP-266
<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-173085
<b>Date Posted</b>	20th April 2026
<b>Versions affected</b>	DDK Releases up to and including 25.3 RTM
<b>Vulnerability</b>	A web page that contains unusual GPU shader code can cause a crash in the GPU shader compiler library. On certain devices, this can enable further exploits on the device.
<b>Resolution</b>	The DDK compiler has been updated to address the issue.

<b>Title</b>	GPU DDK – libusc Stack overflow at DrawArrays and DrawArraysInstanced
<b>Our Reference</b>	PSP-273
<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-172874
<b>Date Posted</b>	20th April 2026

We use cookies to improve your experience and to measure the performance of our website content. You can either consent to accept all the cookies or choose which ones you want.

Change settings

Accept All

<b>Versions affected</b>	DDK Releases starting from REL/24.2 RTM2 up to
<b>Vulnerability</b>	A web page that contains unusual GPU shader code that can cause a crash in the GPU shader compiler library. On certain devices, this could enable for example further denial of service attacks.
<b>Resolution</b>	The DDK compiler library has been updated to handle the crash process executing the shader compilation.

<b>Title</b>	GPU DDK – libufwriter UAF read at llvm::UFWriterV
<b>Our Reference</b>	PSP-349
<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-173618
<b>Date Posted</b>	20th April 2026
<b>Versions affected</b>	DDK Releases up to and including 25.3 RTM
<b>Vulnerability</b>	A web page that contains unusual GPU shader code that can cause a free crash in the GPU shader compiler library. On certain devices, this could enable further exploits on the device.
<b>Resolution</b>	The DDK compiler library has been updated to handle the crash process executing the shader compilation.

<b>Title</b>	GPU DDK – RGXCreateFreeList weakness allows a
<b>Our Reference</b>	PSP-124
<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-159080
<b>Date Posted</b>	20th April 2026
<b>Versions affected</b>	DDK Releases
<b>Vulnerability</b>	Software in the GPU driver that can overflow buffers and cause a crash.
<b>Resolution</b>	The DDK kernel has been updated to handle sensitive buffers.

<b>Title</b>	GPU DDK – libufwriter UAF read at llvm::UFWriterV
<b>Our Reference</b>	PSP-270

We use cookies to improve your experience and to measure the performance of our website content. You can either consent to accept all the cookies or choose which ones you want.

Change settings

Accept All

<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-173080
<b>Date Posted</b>	20th April 2026
<b>Versions affected</b>	DDK Releases up to and including 25.2 RTM
<b>Vulnerability</b>	A web page that contains unusual WebGPU content dereference crash in the GPU GLES user-space shared workload has system privileges this could enable t
<b>Resolution</b>	The DDK GLES user-space shared library has been updated to avoid disruption in the process executing the sha

<b>Title</b>	GPU DDK – Dmabuf imports can be used to create
<b>Our Reference</b>	PSP-307
<b>CVE Reference</b>	None
<b>Originator Reference</b>	PP-173473
<b>Date Posted</b>	20th April 2026
<b>Versions affected</b>	DDK Releases up to and including 25.3 RTM
<b>Vulnerability</b>	Software installed and run as a non-privileged user can access a sensitive buffer carrying physical page addresses
<b>Resolution</b>	The DDK kernel module has been updated to address

**Our Technology**

- Edge AI & Compute
- Edge Graphics Processing
- Ray Tracing
- Functional Safety
- Software Solutions
- Open Access
- Design Optimisation Kit

**Useful Links**

- Career
- Developers
- Newsroom
- Resources
- Blog
- Events
- Driver Vulnerabilities

We use cookies to improve your experience and to measure the performance of our website content. You can either consent to accept all the cookies or choose which ones you want.

Change settings Accept All

[Product Finder](#)

[Contact Imagination](#)

**Our Policies**

[Privacy Policy](#)

[Use of Cookies](#)

[Terms of Use](#)

[Trademarks](#)

[Quality Policy](#)

[Product Security Policy](#)

[Modern Slavery Act](#)

**Stay Connected**

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

[Subscribe](#)



© 2026

Imagination Technologies

We use cookies to improve your experience and to measure the performance of our website content. You can either consent to accept all the cookies or choose which ones you want.

[Change settings](#)

[Accept All](#)