NVIDIA DRIVE OS 6.0.6 Linux

Release Notes

January 2023
Prepared and Provided Under NDA

Table of Contents

Introduction

The NVIDIA DRIVE® OS 6.0 Linux Release Notes are for NVIDIA DRIVE® AGX Orin Development Kits.

Note: **This DRIVE OS and DriveWorks release may only be used for test and development.**

NVIDIA DRIVE® OS is the reference operating system and associated software stack, which includes CUDA, TensorRT, NvMedia, NvStreams, and Developer Tools, designed specifically for developing and deploying autonomous applications on DRIVE AGX-based hardware. DRIVE OS includes the NVIDIA DriveWorks SDK as a foundation for autonomous vehicle (AV) software development. The DriveWorks SDK provides an automotive-grade middleware with accelerated algorithms and versatile tools.

DRIVE OS Development Kits

NVIDIA DRIVE® OS Software Development Kit (SDK) is used to develop DRIVE OS applications for deployment on NVIDIA DRIVE AGX™ based hardware platforms.

NVIDIA DRIVE® OS Platform Development Kit (PDK) is used to adapt NVIDIA DRIVE OS to run on custom hardware based on NVIDIA Automotive SoC (i.e., Orin).

DRIVE OS Base Operating Systems

DRIVE OS Linux “Standard”

DRIVE OS Linux “Standard” is a reference platform based on Ubuntu 20.04 LTS Linux, which is intended for prototyping and development of autonomous vehicle platforms. DRIVE OS Linux is production ready but does not go through the same safety assessment as DRIVE OS QNX for Safety.

Release Highlights

Key Features in this Release

For a complete list of new features and enhancements in this release, see New Features and Enhancements.

- Enhanced PKCS #11 security support
- Logging mechanism of system level events, UART prints, and error codes (experimental)
- Support for PCIe Root-Port (RP) End-Point (EP) support (experimental version of full library).
- Linux Security Hardening improvements

Note:	**5.10 is the default kernel. 5.15 is only sanity tested.**

Deprecations in this Release

There are no deprecations in this release.

Planned Upcoming Changes

The following sections describe planned, upcoming changes.

Summary	Module	Impact
Users who build their SIPL Devblk CDD library on the top of the source files provided by NVIDIA use SerDes source files. These files are non-functional-safety (non FuSa) type of SerDes source files until DRIVE OS 6.0.7.	Camera Core	The plan is to package Funtional safety(FuSa) type of SerDes source files in DRIVE OS 6.0.8. Additionally, for OMS, DMS cameras, which may use VCSEL, the extra driver will be added. The details update/guideline will be provided through DRIVE OS 6.0.8 documentation. For more information, contact your NVIDIA representative.
DRIVE OS will allow applications from different Guest OSes to access the same PKCS#11 token in 6.0.7.	Security	-
Application call-backs functions will be statically configured	API	• Applications can no longer call these APIs to register/un-register application call-backs.

through the configurator. The following APIs will be removed in 6.0.7: • `DMA_register_callback()` • `DMA_register_callback_param()` • `DMA_deregister_callback()` • `DMA_deregister_callback_param()` The following redundant/unused APIs will be removed in 6.0.7: • `DMA_Channel_Update()` • `DMA_Update_Fixed_Pattern_Transfer()`		• Applications must remove calls to these APIs. • Call-back functions will need to be statically configured through DMA CDD configuration tool provided by the AUTOSAR vendor • DMA_Channel_Update() • Applications must remove calls to this API. No functional impact as the same configurations are done in the DMA_Init() API. • Applications will no longer be able to change DMA channel configuration at run-time i.e., all DMA channels will be configured statically. • DMA_Update_Fixed_Pattern_Transfer() • Applications must remove calls to this API if used. This API is expected to be unused.
Users who build their SIPL Devblk CDD library on the top of the source files provided by NVIDIA use SerDes source files. These files are non-functional-safety(non FuSa) type of SerDes source files until DRIVE OS 6.0.7. The plan is to package Functional Safety (FuSa) type of SerDes source files in DRIVE OS 6.0.8 and this update can impact the users. Additionally, for OMS, DMS cameras which may use VCSEL, the extra driver will be added.	Camera Core	The details update/guideline will be provided through the documents for DRIVE OS 6.0.8 release. This is a heads up for the upcoming update; for questions, contact your NVIDIA representative.
Support will be removed to execute KeyOn IST and KeyOff IST in the same boot cycle in DRIVE OS 6.0.7. Execution of KeyIST can still be requested for KeyOn or KeyOff. However, the same test configuration will be used for either. Additonally, there will only be a single test result stored; therefore, to avoid overwriting, the results would need to be requested in between each execution.	Standard	The impact includes a minor change to the NvMCU_ISTManager_RE_Set_ISTConfiguration() API. This API will only accept a value of 1 for the NoOfConfigs parameter. Any other value will result in the API returning an error.
Camera SIPL is making a ABI breaking change in 6.0.7 by removing the following enums: NvSiplNvSciSyncClientType::SIPL_SIGNALER_WAITER NvSiplNvSciSyncObjType::NVSIPL_	Standard	• For SIPL_SIGNALER_WAITER, NVSIPL_EOF_PRESYNCOBJ, NVSIPL_SOF_PRESYNCOBJ: This must be fixed if the enums are being used in place of SIPL_WAITER or SIPL_SIGNALER and NVSIPL_EOFSYNCOBJ, respectively. Otherwise, there should not be any impact.

SOFSYNCOBJ NvSiplNvSciSyncObjType::NVSIPL_EOF_PRESYNCOBJ NvSiplNvSciSyncObjType::NVSIPL_SOF_PRESYNCOBJ The reasoning is as follows: • For SIPL_SIGNALER_WAITER, NVSIPL_EOF_PRESYNCOBJ, NVSIPL_SOF_PRESYNCOBJ: There is no use case where the sync object needs to be treated as both Post and Pre-Fence object types at the same time with the same engine (VI and/or ISP). • For NVSIPL_SOFSYNCOBJ: There is no interface to obtain the fence of the SOF object similar to the one we have for EOF object (INvSIPLBuffer::GetEOFNvSciSyncFence). Considering that we already expose the frameCaptureStartTSC timestamp as part of the ImageMetadata, we do not see a need for users to be able to access the SOF fence.		• Stop using NVSIPL_SOFSYNCOBJ.
In the DRIVE OS 6.0.6 release, the following parameters from NvSIPLClient.hpp header were removed: • NvSiplTimeBase timeBase • NvSiplGlobalTime captureGlobalTimeStamp Since the parameters were removed from the header in this release, the associated data types NvSiplTimeBase and NvSiplGlobalTime from SIPL headers will be removed in 6.0.7. These types are defined here: • https://tegra-sw-opengrok.nvidia.com/source/xref/stage-main_automotive/camera/fusa/	Standard	The NvSiplTimeBase and NvSiplGlobalTime data types will be removed in DRIVE OS 6.0.7.

sipl/include/NvSIPLCommon.hpp#112 https://tegra-sw-opengrok.nvidia.com/source/xref/stage-main_automotive/camera/fusa/sipl/include/NvSIPLCommon.hpp#64		

New Features and Enhancements

This release includes support for these new features and enhancements.

New Features for DRIVE OS

Multicast Capability

DRIVE OS provides the network switch configuration without generating network traffic storm.

PKCS#11 Common Generic Data Object Attributes for CKO_DATA Objects

1. DRIVE OS supports the following PKCS #11 [PKCS11-BASE-v3.0] common generic data object attributes for CKO_DATA objects:
   - CKA_APPLICATION
   - CKA_OBJECT_ID
   - CKA_VALUE
2. DRIVE OS accepts the synch call if the state is De-init.
   - A programming request of a key object can be accepted by the software and buffered in RAM until a point in time where it can be committed to secure storage. In that scenario, reading the return value of the programming request, the user application is not sure if the key object has really been written to secure storage or if it is still buffered in RAM. Users want the option to issue the programming request synchronously, i.e. the API shall not reply with a status until the operation has been completely finished and the key object is programmed in secure storage or the operation failed. Performing the programming request in this fashion results in increased latency for the software performing the programming operation as it has to wait until the Secure NOR is updated to report back the result and hence DRIVE OS only accepts sync call if the state is De-init.
3. When an application is invoked, DRIVE OS will perform the following Cryptographic Key Wrapping mechanisms respectively without exposure of the wrapped Cryptographic Key(s) to the application:

PKCS #11 Functions	**PKCS #11 Mechanisms**	**Key Sizes**
C_WrapKey	CKM_AES_CBC	128 bits
	CKM_NVIDIA_AES_CBC_KEY_DATA_WRAP	128 bits

Early Preview: DRIVE OS Linux SDK/PDK based on Kernel 5.15

Kernel 5.15 based DRIVE OS PDK is available. You must use a separate PDK/SDK/Docker image but install instructions remain the same, with the exception of the bind parameter to include an additional parameter.

Texas Instruments FPD-Link IV

DRIVE OS supports FPD-Link IV serializer/deserializer. The reference system used for FPDLink is the Sony IMX728 120FOV FPD-Link IV camera module and Nvidia camera interface module (CIM) (P3714-B00) installed in the Orin development kit.

- Reference Hardware
  - IMX728 (Sony Model # IMX728EVB-MSH-STM3) with TI UB971 serializer
  - Camera interface module (P3714-B00) with TI UB974 deserializer
  - Orin development kit
- What is provided in the DRIVE OS package?
  - IMX728 (Sony Model # IMX728EVB-MSH-STM3) camera device driver and tuning binaries
  - SERDES driver source code
- What is validated in DRIVE OS with reference hardware?
  - Raw capture with IQ tuning for IMX728 120FOV FPD-Link IV (Sony Model # IMX728EVB-MSH-STM3)
  - Multi camera support (up to 4 cameras) on a single deserializer in C-Phy 4 trios
- What is not validated?
  - Error propagation and decoding
  - Enable and disable link
  - Heterogenous cameras
  - Multiple deserializers active

New raw2rj Format

Note:	- Only applications using DRIVE OS SIPL library (safety camera library) to manage Sony IMX728 or IMX623 cameras and processing RAW bayer data (directly from sensors) are

affected. Users consuming post-processed data from SIPL (post-ISP, after demosaic) are not affected.

- Non-SIPL users are not affected.
- Other camera drivers (including drivers developed by customers themselves) are not affected.

For a 12-bit Bayer image pixel format representation: in addition to left-justified format "raw12" (MSB aligned), a new right-justified format "raw12rj" (LSB aligned with most significant bits padded with 0) was added. raw12rj is used by default for IMX728 and IMX623 SIPL sensor drivers.

Current format "raw12" (left justified):

- Valid bits are left-justified (pixel valid data starts at MSB).
- Most significant bits are replicated in LSBs as a padding.
- e.g., output_t_r16 = (raw12 << 4) | (raw12 >> 8)

New format "raw12rj":

- Valid bits are right-justified.
- Unused most significant bits are padded with 0s.
- e.g., output_t_r16 = (raw12 & 0x0FFF)

PDK

- New inputFormat "raw12rj" is introduced as an option to SIPL json configuration file for camera platform configuration.
- It is a decision of each camera driver which input formats to support.

PCIe RP EP Support

Modules: Safety and Standard

Note: **This experimental version of the full library is available in 6.0.6. The stable version will be supported in 6.0.7.**

The DRIVE OS provides PCIe Controller on each NVIDIA SoC in the following modes:

SNo	Mode	Lane Configuration
1	Root-Port (Bi-directional Data Communication)	x8, x4, x2
2	End-Point (Bi-directional Data Communication)	x8, x4, x2

DRIVE OS provides PCIe controller with following combinations of RP EP connections per Orin SoC:

S No.	RP-EP combination per SOC	Lane Configuration Mode
1	Single RP	x8, x4, x2
2	Single EP	x8, x4, x2

3	Single RP + Single EP	x4, x2
4	Dual RP	x4, x2
5	Dual EP	x4, x2
6	Dual RP + Single EP	x2
7	Single RP + Dual EP	x2

GMAC Operation for Camera Image Authentication Support

DRIVE OS provides a mechanism for verification of an AES-ECB encrypted GMAC (Galois Message Authentication Code) tag calculated on data as required for authenticating image data and embedded data from sensors.

Camera NITO

The camera NITO file path has changed:

Old path: `/opt/nvidia/nvmedia/nit/`

New path: `/usr/share/camera/`

Applications that are currently accessing Camera NITO files using the `/opt/nvidia/nvmedia/nit/` on Linux must update their logic to use the new paths mentioned above.

Ability to Load and Use Keys

DRIVE OS restricts usage of the Critical Security Parameters embedded in the Functional Safety Island PKCS11 Token persisted in Secure Storage to the Hardware Offload Security Engine inside the Functional Safety Island. DRIVE OS restricts usage of the Cryptographic Keys embedded in a Guest OS PKCS11 Token persisted in Secure Storage to the Hardware Offload Security Engine inside the Guest OS Boundary for AES-128-CMAC [FIPS 197][NIST SP 800-38B] only.

Core Elimination

The intent of DRIVE OS core elimination is to allow an application VM to run on all cores, in part by tightly bounding the asynchronous work done by higher-priority servers on any cores. DRIVE OS facilitates Guest VM(s) to fully utilize all CPU Cores in the system, and delegate CPU cycles to the Services and Server VMs as needed.

Support for CPU Events using Virtualization in Safety Debug Overlays

DRIVE OS provides a means to get low-level events from the Hypervisor to enable investigation of performance bottlenecks and debug complex interactions across multiple SW Elements in DRIVE OS Standard Package. DRIVE OS provides an interface to log the following event types in DRIVE OS Standard and Extended Safety Debug Overlay Builds:

4. Non-Secure Kernel (HV) - HV RTOS process context switch events
5. Context switch in and out of TOS

Versioning Info to Bootchains at Partition Level

> **Note:** **The API provides 2 version related capabilities:**
>
> 1. A read-only access to the version of each partition.
> 2. Ability to compare any two versions for a particular partition (i.e., whether a given version is greater, lesser, or equal to current partition version).
>
> The version must be a part of each signed storage partition, rather than partition table, so that it is updated when partition content is updated.

DRIVE OS provides a mechanism in DRIVE Update to extract the current version information included in the active and inactive bootchains and its partitions.

For each of the boot-chain it supports, DRIVE OS includes version information for the entire bootchain, as well as each of the comprised partitions.

Interface for AVB/TSN Configuration

DRIVE OS exposes driver interface to configure necessary parameters for AVB/TSN(IEEE 802.1Qav, Qbv, Qbu) hardware configuration.

EqualLayer

DRIVE OS supports Equal Layer on DLA in TensorRT with the following precision modes, configuration/function combinations for each cell marked with a parameter in the below table.

		A
		Precision Mode INT8
1	Format	NCHW
2	Window Size	[1:8], anisotropic

3	Stride Values	[1:16]

cuDLA as a backend for TensorRT

Modules: Standard

DRIVE OS provides a CUDA Programming based DLA backend for TensorRT to enable a unified model based for inference programming.

Allow Writing FSI Token from CCPLEX

DRIVE OS restricts usage of the critical security parameters embedded in the Functional Safety Island PKCS11 Token persisted in Secure Storage to the Hardware Offload Security Engine inside the Functional Safety Island.

Access Control on Clock

The access control on clock feature is enabled in 6.0.6. A client application that uses any clock IDs must have the custom ability of NvClock/ClockID with its clock IDs as sub-range. Ensure that a client application, if it uses any clocks, has NvClock/ClockID ability with the clock IDs in the security policy file or startup command line.

New Features for DriveWorks 5.10

This release includes support for these new features and enhancements.

New Features and Improvements

- Compute Graph Framework (CGF) operational. CGF allows developers to express their application as nodes of a graph, benefits are easy re-use of nodes, intuitive way to structure complex applications and abstraction for communication and scheduling.
- System Task Manager (STM) scheduler operational
  STM is a static deterministic, non-preemptive scheduler that derives an optimal schedule for CGF graphs, efficiently using Orin's compute engines.
- Vehicle IO feature updated with new data structures.

Installation and Getting Started

- DriveWorks 5.10 is installed with DRIVE OS 6.0.6. No separate installation of DriveWorks libraries are needed.

- Please refer to the Getting Started section of the DriveWorks SDK Reference Documentation for information about how to verify the installation and get started developing with DriveWorks.
- DriveWorks samples and data are not installed on the target OOBE RFS for DRIVE Linux, as they would occupy too much space. Refer to the Getting Started section of the DriveWorks SDK Reference Documentation for information about building and running samples on Orin.

Fixed Issues

The following DRIVE OS and DriveWorks issues from the previous release are resolved in this release:

Feature	Module	Description
3656116	TensorRT builder	**What was the issue?** There was an up to 7% performance regression for the 3D-UNet networks compared to TensorRT 8.4 EA when running in INT8 precision on NVIDIA Orin due to a functionality fix. **How did it impact the customer?** When running 3D-UNet networks in INT8 precision, the latency was up to 7% longer than in TensorRT 8.4 EA. **Was it for SDK/PDK?** SDK
3657753	TensorRT builder	**What was the issue?** There were issues with large channel sizes with structured sparsity convolution kernels (seen at size 4096). **How did it impact the customer?** Computation on the GPU halted unexpectedly in this case. **Was it for SDK/PDK?** SDK
3698054	TensorRT builder	**What was the issue?** In some cases, the TensorRT builder allowed input and output tensors in HWC16 format in FP16 precision. This format was outside the safety scope. **How did it impact the customer?** The TensorRT builder generated safe engines outside the safety scope, which failed consistency check and so should not have been used for inference. **Was it for SDK/PDK?** SDK
200759535	Samples	**What was the issue?** Due to the limitation in the DLA compiler adding copy operators for the bindable inputs, TensorRT builder fell back the concat layer to GPU if any of its input tensors was the input of the DLA subgraph. **How did it impact the customer?** If there was a concat layer in the network and any of its input tensors was the input of the DLA subgraph, the TensorRT builder failed to build the engine when allowGPUFallback was disabled. **Was it for SDK/PDK?** SDK

3263411	DLA	**What was the issue?** For some networks, building and running an engine in the standard runtime would have better performance than the safety runtime. This was due to various limitations in scope of the safety runtime including more limited tactics, tensor size limits, and operations supported in the safety scope. **How did it impact the customer?** Inference in the safety runtime were significantly slower than in the standard runtime. **Was it for SDK/PDK?** SDK
3827883	TensorRT builder	**What was the issue?** The trtexec binary shipped with TensorRT had an unnecessary dependency on deprecated NVMedia libraries. **How did it impact the customer?** The binary was not usable if the deprecated NVMedia libraries were missing. **Was it for SDK/PDK?** PDK
3698033	DLA	**What was the issue?** Some networks failed to build DLA INT8 loadable in DLA_STANDALONE mode with INT8 calibrator. **How did it impact the customer?** When DLA_STANDALONE mode was enabled, when building DLA INT8 loadable, some operators caused unexpected errors when building the engine. **Was it for SDK/PDK?** Standard, SDK
3689094	DLA	**What was the issue?** TensorRT took some dense weights as sparse, if they matched some special pattern. **How did it impact the customer?** For some networks using sparsity, TensorRT produced inaccurate results. **Was it for SDK/PDK?** Standard, SDK
3790584	CGF SAL	CGF Demo tool showed inconsistent behavior. Generates random exit codes. 207, 6, 0 etc.
3746011	CGF	Sample_cgf_camera_interprocess failed with error: Failed with NvSciError_BadParameter(256) in src/dwcgf/channel/impl/ChannelNvSciStream_new.hpp:466
3840993	STM	STM Cross-Compilation binaries generation failed for QNX.
3795934	STM	STM and SSM samples binary were not generating after compilation and cross compilation. sample_image_pyramid_pva was also missing.
200770274	System Software MCU Firmware	**What was the issue?** TMON was powered off before MCU when the board was disconnected from the power supply. Thus, TMON pins go low, which was detected by MCU **How did it impact the customer?** The customer got TMON alerts/notifications on board poweroff/powercycle.
		The following algorithms were not supported on Orin's OFA and/or PVA engines in the previous release: • ImageFilter (Recursive Gaussian Filter, BoxFilter, 2Dconv). • FAST9 Feature Detector, Standard Harris Corner Detector.

		- IC and fastIC Feature Tracker. - DenseOpticalFlow. - Stereo. - Template Tracker.
3477463	Display	**What was the issue?** EGLDevice based sample applications were failing to display their content on DELL 2415b monitor. **How did it impact the customer?** Customers using DELL 2415b were not able to use EGLDevice based applications.
3479678	System Software	**What was the issue?** USB storage devices (Pen drive, hdd) were not immediately automounted when connected; there was a delay of 5-6 minutes before devices were mounted. This was whether hotplug or connected at boot. **How did it impact the customer?** The user needed to wait for USB storage devices to be mounted.
3470744	Graphics	**What was the issue?** Corruption was observed on buffers that were flipped by Weston clients to Weston via eglSwapBuffers. **How did it impact the customer?** Customers observed corruption on Graphics applications that called eglSwapBuffers (EGL/GL).
3410375	Resource Manager	**What was the issue?** Intermittent deadlock in kernel nvhost driver during channel timeout recovery with virtualized nvhost-based engines. **How did it impact the customer?** If the application was triggering timeouts on virtualized nvhost-based engines, nvhost could deadlock and effectively cause a system hang. However, if timeouts were being triggered, the application was already not working correctly and likely the "pipeline is broken".
3605893	Foundation	**What was the issue?** The KeyOn IST test always fails. **How did it impact the customer?** Customer could only run KeyOff IST test.
3562408	Camera Core	**What was the issue?** Frame drops were observed when running nvsipl_camera sample application with more than 2 IMX728 camera modules (8 MP) with display enabled under following conditions: - 4K display is connected -OR- - RAW output was enabled (--enableRawOutput command line option to nvsipl_camera) **How did it impact the customer?** Customers observed similar frame drops with their camera applications if they used a similar pipeline and had a 4K display connected with more than 2 camera modules of 8MP or higher.

		Was it for SDK/PDK? Linux AV+L
3591349	Docker	**What was the issue?** DRIVE OS 6.0 included the Docker runtime as part of the RFS and so Docker is now available in the Guest OS. However, the runtime was unable to access the internet. **How did this impact the customer?** The customer was unable to perform a subset of basic Docker-related actions, such as pulling and pushing images.
200765598	Virtualization	**What was the issue?** Warm/Guest OS reboot (i.e., “sudo reboot”) was not supported on AV+L/Linux platform for DRIVE OS 6.0/Orin. **How did it impact the customer?** Customer was not able to use the traditional command to reboot the Linux Guest OS alone.
3506785	System Software	**What was the issue?** SOC_ERROR was asserted by ORIN due to errors in SOC. However, SOC_ERROR assertion was a decision by SEH and for SEH was only sample implementation; hence, suggested customers to look for notification as primary expected results. SOC_ERROR Pin need not be monitored. However, all error notifications should have been tracked. **How did it impact the customer?** Customer had to handle SOC_ERRORs in customers implementation of SEH decide SOC_ERROR Assertion. **Was it for SDK/PDK?** All
3622118	Bootburn	**What was the issue?** New DRIVE AGX Orin Devkit boards taken out of box failed a new flashing process if you attempted to flash before the EULA was accepted on the DevKit. **Was it for SDK/PDK?** All
3664355	Yocto	**What was the issue?** Yocto tegra-initramfs-recovery build failed if the PDK packages were not installed. **How did it impact the customer?** Customers who installed SDK-only Debians and build Yocto tegra-initramfs-recovery image hit a build failure. However, the Recovery initramfs was for the PDK package only, and required PDK packages to be installed. **Was it for SDK/PDK?** All.
200454454	Clocks	**What was the issue?** Switching AXI CBB to PLLC2 (202 Mhz) as per POR causing (benchmark, memory etc) test failures. **How did it impact the customer?** You saw high CBB performance as it is on PLLP (405MHz) than as per POR

		(PLLC2/ -> ~202MHz) for 55W profile. **Was it for SDK/PDK?** All
3709711	Camera Core	**What was the issue?** The SIPL and FuSa UMD libraries emitted Capture Status Timeout error logs at Deinitialization if the StopModule API was implemented for the sensor driver. **How did it impact the customer?** The Capture Status Timeout error logs were benign and did not have any safety impact. **Was it for SDK/PDK?** The issue with the Capture Status Timeout error logs was present in all the above packages where the sensor driver implemented the StopModule API.
		What was the issue? The StopModule API had not been implemented in the AR0820 and OV2311 sensor drivers. At Deinitialization, the sensors did not receive a command to gracefully stop streaming, and instead continued transmitting data until the power was disabled. **How did it impact the customer?** The customer saw SEH error logs to the AURIX and CCPLEX UART terminals due to CSI pixel data continuing to be transmitted to Tegra despite the capture pipeline(s) having already been arrested. SEH logs were reported to the application. **Was it for SDK/PDK?** The issue affected the standard build for the AR0820 sensor and OV2311 sensor, for both the SDK and PDK for both sensors.
3465334	MCU Firmware	**What was the issue?** VRS12 did power-down sequence verification of rails during power off. The power-down sequence of rails was not consistent for every power-off cycle, thus leading to intermittent fault during power-off sequence verification. **How did it impact the customer?** The customer got VRS12 power-down sequence failures during power-off. This broke voltage monitoring safety recommendations
3698410	Camera Core	**What was the issue?** After starting nvsipl_camera application, 1 - HW error (Code - 0x28b6) was reported from VI error collator . These error reports interrupted FSI and errors were processed and notified to system error handler on FSI. **How did it impact the customer?** Error was seen by customer, but there was no functional impact and happened only the first few times after boot. Quality and throughput of images were not impacted in runtime. **Was it for SDK/PDK?** PDK.
3734112	DRIVE Update	**What was the issue?** DUPKG tool errored out when provided an absolute path for the "--out" argument. **How did it impact the customer?** Customer were not able to generate the package if an absolute path was

		provided to "--out" argument. **Was it for SDK/PDK?** All
3609001	IST	**What was the issue?** Some KeyIST configuration values were not POR value. **How did it impact the customer?** The KeyIST diagnostic ran longer the POR KPIs. In very rare conditions, the diagnostic reported a false failure. **Was it for SDK/PDK?** All
3626664	Safety Services	**What was the issue?** The security settings of error collators in PSC were set up such that only PSC could access the same. This was an exception to Global Rule that all Error Collators should be accessible only by FSI. During Fault injection testing, when an error was injected, FSI SW attempted to access Error Collators in PSC and Crashes with an illegal access exception. The Affected Fault names related to ECs in PSC were: PSC_CLUSTER_UE PSC_SE_UE PSC_DMA_UE PSC_FABRIC_UE PSC_AON_UE PSC_SE_CE PSC_DMA_CE PSC_CLUSTER_CE PSC_FABRIC_CE PSC_AON_CE PSC_FABRIC_AON_UE PSC_FABRIC_AON_CE CAR_PSC_UE PADCTL_PSC_G8_UE **How did it impact the customer?** Whenever there was an Error in PSC reported via Error Collators, FSI would also have an exception. The customer was not able to perform fault injection testing. However, SOC_ERROR would be asserted by HW, which could be detected by MCU SW. MCU would also observe SPI E2E error as FSI would crash (@shubhamj to Confirm the same) **Was it for SDK/PDK?** All
3727547	BPMP	Safe shutdown timeout happened in simulated safe poweroff MCU shell command (fails on P3663, but PASS on P3710).
3664337	System Software	**What was the issue?** DemoAppCom assumed that the current user (that was executing the app) was a member of the group nvfsicom,nvepl. The group nvfsicom already existed in

		the filesystem, but the membership was not. The permission occured due to 2 reasons: Filesystem user account did not have nvfsicom,nvepl memberships preset. The instructions to execute DemoAppCom did not update the memberships of the user account before executing the app. **How did it impact the customer?** DemoAppCom failed to launch and reported permission denied. **Was it for SDK/PDK?** Standard SDK
3664734	System Software	**What was the issue?** DemoAppCom assumed that the current user (that was executing the app) was a member of the group nvfsicom,nvepl. The group nvfsicom already existed in the filesystem, but the membership was not. The permission occured due to 2 reasons: Filesystem user account did not have nvfsicom,nvepl memberships preset. The instructions to execute DemoAppCom did not update the memberships of the user account before executing the app. **How did it impact the customer?** DemoAppCom failed to launch and reported permission denied. **Was it for SDK/PDK?** Standard SDK
3708327	Yocto	**What was the issue?** Weston launch failed due to failure in loading drm-backend.so. **How did it impact the customer?** Customers using Weston needed to apply a patch and rebuild it. **Was it for SDK/PDK?** All.
3710589	Camera Core	**What was the issue?** Frame Discontinuities were observed when running nvsipl_camera sample application with more than 2 IMX728 camera modules (8 MP) with display enabled under following condition: 3 ISP outputs were enabled simultaneously (none of the --disableISP0Output, --disableISP1Output or --disableISP2Output are specified). **How did it impact the customer?** Customer could only use 2 ISP outputs from each camera for display when using 3 or more 8MP cameras. **Was it for SDK/PDK?** Issue was observed on Embedded Linux AV+L PDK/SDK.
3719548	DRIVE Update	**What was the issue?** DRIVE Update decompressor did not handle abort, calling abort during deploy would lock up decompressor if it was used in deployment. **How did it impact the customer?** Deployment with decompressor could not be aborted. **Was it for SDK/PDK?** All

3730926	Security	11 sub-tests of PKCS#11 test suite failed on ODM fused board.
3535820	Security	**What was the issue?** FSI did not have access to EMC registers for: • Enabling DRAM uncorrected error reporting • Reading bad page information and handling DRAM uncorrected errors **How did it impact the customer?** DRAM ECC uncorrected error could not be handled and system continues to operate with DRAM ECC uncorrected error, which is unsafe. **Was it for SDK/PDK?** All
3722779	AURIX	**What was the issue?** SC7 exit failed intermittently on a few boards. **How did it impact the customer?** Customers saw SC7 exit failure intermittently and needed to perform aurixreset to recover from SC7 state. **Was it for SDK/PDK?** All.
3820323	Security	**What was the issue?** The PKCS#11 Library had allowed CKA_LABEL attribute template entries to be shorter than 32 bytes and to contain NULL characters. In 6.0.5.0, checks were enforced to ensure CKA_LABEL content is 32 bytes, space padded to fill the entire field if necessary, and did not contain NULL. **How did it impact the customer?** Attempts to generate, create, copy, derive or C_SetAttributeValue keys with non-compliant CKA_LABEL template attributes were rejected in 6.0.5.0 release. **Was it for SDK/PDK?** All
3786483	Security	**What was the issue?** The PKCS#11 Library documentation had been updated to allow you to set the CKA_SENSITIVE value in the template for the derived key, default TRUE if not. However, if you attempted to derive a key with CKA_SENSITIVE False, the request was denied. **How did it impact the customer?** Could not derive a key with CKA_SENSITIVE attribute False. **Was it for SDK/PDK?** SDK
3770879	Camera	**What was the issue?** In Linux, registering a signaler NvSciSyncObj with the INvSIPLClient::ConsumerDesc::OutputType::ICP output of a SIPL pipeline could have lead to a kernel panic. Please note that in this case a signaler NvSciSyncObj was defined as a synchronization object of any NvSiplNvSciSyncObjType other than NVSIPL_PRESYNCOBJ. **How did it impact the customer?** A kernel panic occurred and if it did, the system crashed. **Was it for SDK/PDK?**

		All
3836840	NVSCI	**What was the issue?** Customers saw "[ERROR: OutputFnObjDesc]: Failed to create Object from export descriptor." error print while using NvStreams C2C feature, although this error code was handled internally by NvSciStream and was not propagated to application. Hence, there was no impact or action required from the customer application. **How did it impact the customer?** This error print might have mislead customers as there was no error propagated to application for this error. **Was it for SDK/PDK?** All
3811254	System Software	**What was the issue?** On earlier versions of P3710-SKU10/SKU12 TS1, TS2, TS3, TS4, the PCIE retimer used for C2C was intermittently held in reset. **How did it impact the customer?** Customer saw failures when trying to manually update. This also manifested as failures to connect via C2C. **Was it for SDK/PDK?** Standard SDK/PDK only.
3411978	Bootburn	**What was the issue?** DRIVE OS 6.0.5.0 had a new feature to add versioning info to bootchains at the partition level for DRIVE Update to identify the current version. However, in 6.0.5.0, only full updates were supported. Partial updates were not supported. **How did it impact the customer?** You were not able to update target images selectively with the -u option. **Was it for SDK/PDK?** All
3837369	MCU Firmware	**What was the issue?** On P3663 and 3710 boards with an ES sample of VRS11, VRS11-1 (one of the VRS11) was not accessible for configuration until Tegra booted up as EN signal for this chip was controlled by Tegra and it was only set once Tegra booted up. Accessing the I2C channel before the client was up sometimes caused the I2C driver to hang. This issue (driver hang) was seen on 2 P3663 boards out of 4 boards, and only in IST mode. **How does it impact the customer?** Software hung during bootup during IST mode. **Was it for SDK/PDK?** All
3313449	Virtualization	**What was the issue?** For Orin devices connected over NvSciC2C connection, if one Orin unexpectedly resets or shuts down, the other Orin showed CBB timeout prints and hung. **How did it impact the customer?** Unexpected reset/shutdown of one side of the link brought down the system. **Was it for SDK/PDK?**

		All
3681090	MCU Firmware	**What was the issue?** On P3663 boards with a VRS10 ES sample, VRS-10 ES asserted NIRQ if NRST was pulled low externally. When the SOC_PWR_ON was set to HIGH, the VRS10 released the SoC reset (NRST) but it was held by MCU, and thus VRS10 detected that as an error. **How did it impact the customer?** There was no functional impact as Orin booted up even on this error. However, safety requirements were breached. **Was it for SDK/PDK?** All
200782948	SAL	Lraw recording replay failed. However, raw/mp4 replay was unaffected.
3837042		Recorder: MP4 Recording with quality=[1/20/50] fails, DW_NVMEDIA_ERROR: EncoderNvMedia: error getting encoded data : 9
3837023		[B] Recorder Tool : Playback of H265 Recording with isp-mode=yuv420-uint8-bl & quality [1/20/50] hangs
3795061		Recorder and replayer tool with rig file fails with error: 'dw::core::OutOfBoundsException' what(): HashMap: Index not found
3499987		Lidar chop process got stuck for an infinite time.
3597225		Video exporter and header-dump tool dumped segmentation fault while exiting.
3605267		sample_cgf_dwchannel was failing for hybrid inter-process, inter-chip scenario and sync_mode p2c, and it was giving a segmentation fault.
3478783	Image and Cloud Processing	sample_image_pyramid_pva with 8MP camera input failed; other resolutions were supported.
3478840		sample_feature_descriptor with raw video input failed, Fast9 task submission failed: PvaError_Error.
3597551		Sample_feature_tracker with PVA Detector failed to run, DW_NOT_AVAILABLE: FeatureDetectPipelinePVA: PVA was not available on this platform.
3558283		LRAW recording playback gave blank output, and both raw and lraw playback failed to exit gracefully. You needed to kill the playback.
3432606		DriveWorks exception was thrown: DW_INVALID_HANDLE: Cannot cast to C++ handle when exiting "sample_image_streamer_cross".
3823785	DNN Framework	[B]TensorRT_optimization tool Failed to parse ONNX model from file: ../../data/samples/detector/weights.onnx
200776376	General	All samples dumped error on console: TimeSource Eth: PTP ioctl returned error. Synchronized time was not available from this timesource.
3401171		DW_GL_ERROR was visible in multiple samples applications.
3831376	CGF	run_cgf.sh tool exited with launcher exit status: 6.
3835079		run_cgf demo fails to launch with exit status “33” and “[STM][ERROR] Failed to receive mqueue message; errno: 4 (Interrupted system call)”

NVIDIA Software Security Updates

This release of NVIDIA DRIVE OS 6.0 Linux includes updates that address the following issue[s]:

CVE ID	NVIDIA Issue Number	Description
Not Assigned	3769227	NVIDIA Tegra kernel driver for Linux contains a vulnerability in NVIDIA camera, where a local attacker with regular user privilege can take advantage of failure to validate input from untrusted source , possibly leading to limited Denial of Service.
CVE-2022-2309	3840236	NULL Pointer Dereference allows attackers to cause a denial of service (or application crash). This only applies when lxml is used together with libxml2 2.9.10 through 2.9.14. libxml2 2.9.9 and earlier are not affected. It allows triggering crashes through forged input data, given a vulnerable code sequence in the application. The vulnerability is caused by the iterwalk function (also used by the canonicalize function). Such code shouldn't be in wide-spread use, given that parsing + iterwalk would usually be replaced with the more efficient iterparse function. However, an XML converter that serialises to C14N would also be vulnerable, for example, and there are legitimate use cases for this code sequence. If untrusted input is received (also remotely) and processed via iterwalk function, a crash can be triggered.
CVE-2022-2068	3840236	In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in

		OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).
CVE-2022-1292	3840236	The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).
CVE-2022-2097	3840236	AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).
CVE-2022-0778	3840236	The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use

		the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).
CVE-2021-4160	3840236	"There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).
CVE-2021-3711	3840236	In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen"

		parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).
CVE-2021-3712	3840236	ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data"

		field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).
CVE-2020-1971	3840236	The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this

		attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).
CVE-2022-0563	3840236	A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.
CVE-2021-3996	3840236	"A logic error was found in the libmount library of util-linux in the function that allows an unprivileged user to unmount a FUSE filesystem. This flaw allows a local user on a vulnerable system to unmount other users' filesystems that are either world-writable themselves (like /tmp) or mounted in a world-writable directory. An attacker may use this flaw to cause a denial of service to applications that use the affected filesystems
CVE-2021-3995	3840236	"A logic error was found in the libmount library of util-linux in the function that allows an unprivileged user to unmount a FUSE filesystem. This flaw allows an unprivileged local attacker to unmount FUSE filesystems that belong to certain other users who have a UID that is a prefix of the UID of the attacker in its string form. An attacker may use this flaw to cause a denial of service to applications that use the affected filesystems
CVE-2021-37600	3840236	An integer overflow in util-linux through 2.37.1 can potentially cause a buffer overflow if an attacker were able to use system resources in a way that leads to a large number in the /proc/sysvipc/sem file. NOTE: this is unexploitable in GNU C Library environments, and possibly in all realistic environments.
CVE-2022-1586	3840236	An out-of-bounds read vulnerability was discovered in

		the PCRE2 library in the compile_xclass_matchingpath() function of the pcre2_jit_compile.c file. This involves a unicode property matching issue in JIT-compiled regular expressions. The issue occurs because the character was not fully read in case-less matching within JIT.
CVE-2022-1587	3840236	An out-of-bounds read vulnerability was discovered in the PCRE2 library in the get_recurse_data_length() function of the pcre2_jit_compile.c file. This issue affects recursions in JIT-compiled regular expressions caused by duplicate data transfers.
CVE-2021-28153	3840236	NVIDIA Tegra kernel driver or Windows/Linux GPU Display Driver contains a vulnerability in component i.e. NVHost, NVMAP, NVIDIA camera or the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where CWE description (see below text), which may lead to impact from the impact field.
CVE-2021-27219	3840236	"An issue was discovered in GNOME GLib before 2.66.6 and 2.67.x before 2.67.3. The function g_bytes_new has an integer overflow on 64-bit platforms due to an implicit cast from 64 bits to 32 bits. The overflow could potentially lead to memory corruption
CVE-2021-27218	3840236	An issue was discovered in GNOME GLib before 2.66.7 and 2.67.x before 2.67.4. If g_byte_array_new_take() was called with a buffer of 4GB or more on a 64-bit platform, the length would be truncated modulo 2**32, causing unintended length truncation.
CVE-2022-35252	3840236	When curl is used to retrieve and parse cookies from a HTTP(S) server, itaccepts cookies using control codes that when later are sent back to a HTTPserver might make the server return 400 responses. Effectively allowing a"sister site" to deny service to all siblings.
CVE-2022-32221	3840236	"When doing HTTP(S) transfers, libcurl might erroneously use the read callback (`CURLOPT_READFUNCTION`) to ask for data to send, even when the `CURLOPT_POSTFIELDS` option has been set, if the same handle previously was used to issue a `PUT` request which used that callback. This flaw may surprise the application and cause it to misbehave and either send off the wrong data or use memory after free or similar in the subsequent `POST` request. The problem exists in the logic for a reused handle when it is changed from a PUT to a POST

CVE-2022-32208	3840236	"When curl < 7.84.0 does FTP transfers secured by krb5, it handles message verification failures wrongly. This flaw makes it possible for a Man-In-The-Middle attack to go unnoticed and even allows it to inject data to the client.
CVE-2022-32206	3840236	curl < 7.84.0 supports "chained" HTTP compression algorithms, meaning that a serverresponse can be compressed multiple times and potentially with different algorithms. The number of acceptable "links" in this "decompression chain" was unbounded, allowing a malicious server to insert a virtually unlimited number of compression steps.The use of such a decompression chain could result in a "malloc bomb", makingcurl end up spending enormous amounts of allocated heap memory, or trying toand returning out of memory errors.
CVE-2022-27782	3840236	libcurl would reuse a previously created connection even when a TLS or SSHrelated option had been changed that should have prohibited reuse.libcurl keeps previously used connections in a connection pool for subsequenttransfers to reuse if one of them matches the setup. However, several TLS andSSH settings were left out from the configuration match checks, making themmatch too easily.
CVE-2022-27781	3840236	"libcurl provides the `CURLOPT_CERTINFO` option to allow applications torequest details to be returned about a server's certificate chain.Due to an erroneous function, a malicious server could make libcurl built withNSS get stuck in a never-ending busy-loop when trying to retrieve thatinformation
CVE-2022-27776	3840236	A insufficiently protected credentials vulnerability in fixed in curl 7.83.0 might leak authentication or cookie header data on HTTP redirects to the same host but another port number.
CVE-2022-27775	3840236	An information disclosure vulnerability exists in curl 7.65.0 to 7.82.0 are vulnerable that by using an IPv6 address that was in the connection pool but with a different zone id it could reuse a connection instead.
CVE-2022-27774	3840236	An insufficiently protected credentials vulnerability exists in curl 4.9 to and include curl 7.82.0 are affected that could allow an attacker to extract credentials when follows HTTP(S) redirects is used with authentication could leak credentials to other services

NVIDIA CONFIDENTIAL

		that exist on different protocols or port numbers.
CVE-2022-22576	3840236	An improper authentication vulnerability exists in curl 7.33.0 to and including 7.82.0 which might allow reuse OAUTH2-authenticated connections without properly making sure that the connection was authenticated with the same credentials as set for this transfer. This affects SASL-enabled protocols: SMPTP(S), IMAP(S), POP3(S) and LDAP(S) (openldap only).
CVE-2021-22947	3840236	When curl >= 7.20.0 and <= 7.78.0 connects to an IMAP or POP3 server to retrieve data using STARTTLS to upgrade to TLS security, the server can respond and send back multiple responses at once that curl caches. curl would then upgrade to TLS but not flush the in-queue of cached responses but instead continue using and trustingthe responses it got *before* the TLS handshake as if they were authenticated.Using this flaw, it allows a Man-In-The-Middle attacker to first inject the fake responses, then pass-through the TLS traffic from the legitimate server and trick curl into sending data back to the user thinking the attacker's injected data comes from the TLS-protected server.
CVE-2021-22946	3840236	A user can tell curl >= 7.20.0 and <= 7.78.0 to require a successful upgrade to TLS when speaking to an IMAP, POP3 or FTP server (`--ssl-reqd` on the command line or`CURLOPT_USE_SSL` set to `CURLUSESSL_CONTROL` or `CURLUSESSL_ALL` withlibcurl). This requirement could be bypassed if the server would return a properly crafted but perfectly legitimate response.This flaw would then make curl silently continue its operations **withoutTLS** contrary to the instructions and expectations, exposing possibly sensitive data in clear text over the network.
CVE-2021-22925	3840236	"curl supports the `-t` command line option, known as `CURLOPT_TELNETOPTIONS`in libcurl. This rarely used option is used to send variable=content pairs toTELNET servers.Due to flaw in the option parser for sending `NEW_ENV` variables, libcurlcould be made to pass on uninitialized data from a stack based buffer to theserver. Therefore potentially revealing sensitive internal information to theserver using a clear-text network protocol.This could happen because curl did not call and use sscanf() correctly whenparsing the string provided by the application.
CVE-2021-	3840236	"libcurl keeps previously used connections in a

22924		connection pool for subsequenttransfers to reuse, if one of them matches the setup.Due to errors in the logic, the config matching function did not take 'issuercert' into account and it compared the involved paths *case insensitively*,which could lead to libcurl reusing wrong connections.File paths are, or can be, case sensitive on many systems but not all, and caneven vary depending on used file systems.The comparison also didn't include the 'issuer cert' which a transfer can setto qualify how to verify the server certificate
CVE-2021-22898	3840236	curl 7.7 through 7.76.1 suffers from an information disclosure when the `-t` command line option, known as `CURLOPT_TELNETOPTIONS` in libcurl, is used to send variable=content pairs to TELNET servers. Due to a flaw in the option parser for sending NEW_ENV variables, libcurl could be made to pass on uninitialized data from a stack based buffer to the server, resulting in potentially revealing sensitive internal information to the server using a clear-text network protocol.
CVE-2021-22890	3840236	curl 7.63.0 to and including 7.75.0 includes vulnerability that allows a malicious HTTPS proxy to MITM a connection due to bad handling of TLS 1.3 session tickets. When using a HTTPS proxy and TLS 1.3, libcurl can confuse session tickets arriving from the HTTPS proxy but work as if they arrived from the remote server and then wrongly "short-cut" the host handshake. When confusing the tickets, a HTTPS proxy can trick libcurl to use the wrong session ticket resume for the host and thereby circumvent the server TLS certificate check and make a MITM attack to be possible to perform unnoticed. Note that such a malicious HTTPS proxy needs to provide a certificate that curl will accept for the MITMed server for an attack to work - unless curl has been told to ignore the server certificate check.
CVE-2021-22876	3840236	curl 7.1.1 to and including 7.75.0 is vulnerable to an "Exposure of Private Personal Information to an Unauthorized Actor" by leaking credentials in the HTTP Referer: header. libcurl does not strip off user credentials from the URL when automatically populating the Referer: HTTP request header field in outgoing HTTP requests, and therefore risks leaking sensitive data to the server that is the target of the second HTTP request.

For more information about NVIDIA's vulnerability management, refer to the NVIDIA Product Security page.

Known Limitations

The following sections describe known limitations in 6.0.

Feature	Module	Description
CUDA	CUDA	CUDA CUB (CUB: Main Page (nvlabs.github.io)) is provided as-is and not explicitly supported on NVIDIA DRIVE OS 6.0, although present in the CUDA 11.4 installation. Any risk or liability associated with the usage of CUDA CUB is the responsibility of the customer.
DriveWorks	DNN	Framework samples are not working for caffe based DNNs.
DriveWorks	RAW/LRAW	RAW/LRAW recording is not operational. Please record .mp4 or .h264 instead or use change to DriveWorks 5.8 release.

Known Issues

Note: Due to the introduction of enhanced persistent partition workflow, if you are upgrading from DRIVE OS 6.0.4 to the current DRIVE OS version and using `-init` persistent partitions, follow all the steps mentioned under the Data Migration for Persistent Partitions chapter in the *DRIVE OS 6.0 Linux SDK Developer Guide*.

These are issues discovered during development and QA and are scheduled to be resolved in a future release.

Feature	Module	Description
3928121	NvSCI	**What is the issue?** NvSciBufObjIpcImport() fails to import NvSciBufObj via NvSciIpcEndpoint when it has a similar name as the exporter NvSciIpcEndpoint. **How does it impact the customer?** You cannot share memory objects or do streaming between NvSciIpcEndpoint pairs with similar names in nvsciipc.cfg (i.e., by adding a postfix). **If there is a workaround, what is it?** Do not use similar endpoint name in nvsciipc.cfg (i.e., by adding a postfix. For example, test_endpoint1, test_endpoint10). **When can we expect the fix?** 6.0.6.1 **Is it for SDK/PDK?** All
3947206	NvIPC	**What is the issue?** During guest OS boot, nvsciipc_init is terminated without creating resources due to nvsciipc.cfg configuration file parsing error. **How does it impact the customer?** Applications or services using NvSciIpc are not launched completely due to missing resources and the system does not work properl. The impact is minor once the workaround is implemented. **If there is a workaround, what is it?** Do not add a new line (empty line) in the end or middle of nvsciipc.cfg configuration file. **When can we expect the fix?** 6.0.6.1 **Is it for SDK/PDK?** All

3932674	Camera Core	**What is the issue?** The SIPL camera sample applications IMX728 FPD-Link 2-lane camera module configuration (IMX728_FPDLINK_RGGB_CPHY_x2) fails to initialize and begin streaming. **How does it impact the customer?** Unable to use the IMX728 FPD-Link 2-lane camera module configuration (IMX728_FPDLINK_RGGB_CPHY_x2) in SIPL camera sample applications. They will be able to use the 4-lane IMX728_FPDLINK_RGGB_CPHY_x4 configuration, however. **When can we expect the fix?** The fix is being merged to the development branch and will be present in DRIVE OS 6.0.7.0. **Is it for Standard/Safety, SDK/PDK?** TI FPD-Link support is only present in the standard build, this configuration is not documented in the SDK or PDK.
3957257	System Software	**What is the issue?** Due to build-FS tool issues SDKM update process done by Build-FS to set up the user account removes the filesystem manifest information (and also the manifest filename that indicates the variant of the filesystem). **How does it impact the customer?** After SDKM installation, if the user checks the directory /etc/nvidia/rootfilesystem-manifest will see the following files: • tmp.MANIFEST.json • driveos-rfs.MANIFEST.json (symlink pointing to tmp.MANIFEST.json) Without SDK installed (which is in pre-flash boards) the user checking the directory /etc/nvidia/rootfilesystem-manifest will see the following files: • driveos-oobe-desktop-ubuntu-20.04-rfs.MANIFEST.json • driveos-rfs.MANIFEST.json (symlink pointing to driveos-oobe-desktop-ubuntu-20.04-rfs.MANIFEST.json) **If there is a workaround, what is it?** • The filesystem flashed by SDKM is the same pointed to my symlink: $NV_WORKSPACE/drive-linux/filesystem/targetfs.img. Please use readlink as below to find the target image's filename under the directory $NV_WORKSPACE/drive-linux/filesystem/targetfs-images/ which the symlink $NV_WORKSPACE/drive-linux/filesystem/targetfs.img points to. The filename shows the filesystem type. • readlink -f $NV_WORKSPACE/drive-linux/filesystem/targetfs.img • which returns readlink -f $NV_WORKSPACE/drive-linux/filesystem/targetfs-images/<filename> • The <filename> and filesystem type is given below: • driveos-core-ubuntu-20.04-rfs.img => DRIVE OS Core RFS • driveos-oobe-ubuntu-20.04-rfs.img => DRIVE OS OOBE RFS • driveos-oobe-desktop-ubuntu-20.04-rfs.img => DRIVE OS Desktop RFS • More information on each type is at http://sw-mobile-docs/DRAFT/V6L_ORIN_SDK/common/topics/sys_components/LinuxFilesystems1.html. **When can we expect the fix?**

		6.0.7 **Is it for SDK/PDK?** All
3751073	System Software	**What is the issue?** Hardware limitation (PMIC and Board design) where an older revision of P3663 and P3710 cannot support SC7. P3663-A03, P3710-TS3 and P3710-TS5 or later revisions will only support SC7. **How does it impact the customer?** You cannot use older revision of the board for SC7 testing. **If there is a workaround, what is it?** N/A When can we expect the fix? N/A **Is it for Standard/Safety, SDK/PDK?** All
3952902	IST	**What is the issue?** KIST reports failure with Linux Kernel 5.15 **How does it impact the customer?** You cannot use KIST with 5.15 kernel (kernel-5.10 is working). **If there is a workaround, what is it?** N/A **When can we expect the fix?** 6.0.6.1 **Is it for SDK/PDK?** PDK
3950134	Safety MCU Firmware	**What is the issue?** On the P3663-TS3 board, SAFETY_NIRQ is low during SC7 exit, which leads to the error print "ERROR: MCU_PLTFPWRMGR: Request Orin SC7 Exit failed!. As this is a safety check, it has no functional impact **How does it impact the customer?** You see error print "ERROR: MCU_PLTFPWRMGR: Request Orin SC7 Exit failed!" though SC7 exit is successful. As this is a safety check, it has no functional impact. **If there is a workaround, what is it?** N/A **When can we expect the fix?** As the issue is seen on only a particular board, analysis/fix will take more time and it is planned to be completed by 6.0.7. **Is it for Standard/Safety, SDK/PDK** All
3895994	System Software	**What is the issue?** SC7 Suspend->Resume causes hang intermittently. Issue seen once in 25 cycles of Suspend-Resume. Issue occurs if suspend-resume is triggered in a loop. **How does it impact the customer?**

		System will be in hang state if this issue is hit **If there is a workaround, what is it?** Need a power reset to come out of this state **When can we expect the fix?** 6.0.7 **Is this Standard?** Issue is seen on Linux, PCT Configuration : AV+L **Is it for SDK/PDK?** All
3852875	Camera	**What is the issue?** The PDK source build breaks due to the migration of the NvMedia core header to a 6.x version. **How does it impact the customer?** You are unable to build camera device drivers from source. **If there is a workaround, what is it?** Apply patches to add back nvmedia_core.h header and remove the libnvmedia dependency. Contact your NVIDIA software support representative to obtain the patches. **When can we expect the fix?** 6.0.7 **Is it for SDK/PDK?** All
3839935	IST	**What is the issue?** Some systems fail KIST. **How does it impact the customer?** You may see false KIST failures on some systems. **If there is a workaround, what is it?** No **When can we expect the fix?** 6.0.7 **Is it for SDK/PDK?** PDK
3837369	Safety MCU Firmware	**What is the issue?** MCU software hangs due to I2C transactions during IST. So far, the issue is seen only on two P3663 boards. There is a provided workaround by delaying consecutive VRS10 and 11 I2C transition. **How does it impact the customer?** Board hangs during AURIX bootup. **If there is a workaround, what is it?** You can add a delay between two I2C transitions(as done as part of this workaround) if they are using Infineon iLLD. As the issue is not seen with the Vector I2C driver, you can also switch to the Vector I2C driver as an alternative solution. Enable AFW_I2C_DRV_VECTOR on using Vector I2C driver.

		When can we expect the fix? It is planned to switch to Vector driver in 6.0.6 as this is one of the alternatives to fix the issue. **Is it for SDK/PDK?** All
3558625	IST	**What is the issue?** The Key On IST test sometimes fails the first execution after flashing a new build on Orin. Subsequent tests are expected to pass. **How does it impact the customer?** The first Key On IST run after flashing may fail. You should ignore the first KIST test after flashing if it fails. **If there is a workaround, what is it?** Ignore the first Key On IST test after flashing. **When can we expect the fix?** 6.0.7 **Is it for SDK/PDK?** All
3854952	DRIVE Update	**What is the issue?** DRIVE Update deploy fails with delay greater than 10s in reboot.json. **How does it impact the customer?** There is no max delay documented anywhere, which may cause customer DRIVE Update deploy fail. **If there is a workaround, what is it?** Maximum value of delay in reboot.json is 10s. **When can we expect the fix?** No fix. Avoid the DRIVE Update deploy failure caused by an inappropriate delay value. **Is it for SDK/PDK?** All
3830784	Camera	**What is the issue?** In Reprocess mode, the timestamps - frameCaptureTSC and frameCaptureStartTSC that could be optionally provided as inputs to NvSIPLImageGroupWriter::RawBuffer struct show up swapped as frameCaptureStartTSC and frameCaptureTSC when read from corresponding fields of INvSIPLClient::ImageMetaData from the output buffer. **How does it impact the customer?** Only in reprocess mode the customer will not be able to see the programmed SOF and EOF timestamps properly in the output buffer metadata. **If there is a workaround, what is it?** If necessary, use the frameCaptureTSC/frameCaptureStartTSC in NvSIPLImageGroupWriter::RawBuffer struct swapped. **When can we expect the fix?** 6.0.7 **Is it for SDK/PDK?** All

3640535	Provisioning	**What is the issue?** UFS Memory must be provisioned for performance enhancements. The value for bProvisioningType has changed in the NVIDIA reference board UFS provisioning file, from "0 -- Thin Provisioining Disabled" to "3 -- Thin Provisioning enabled with TPRZ". For more information, refer to the To provision a UFS device through the flashing tools chapter in the *NVIDIA DRIVE OS 6.0 Linux Developer Guide*. As per the UFS Jdec spec JESD220D: bProvisioningType shall be set to configure the logical unit provisioning type 00h: to disable thin provisioning, 5534 02h: to enable thin provisioning with TPRZ = 0 03h: to enable thin provisioning with TPRZ = 1. The "bProvisioningType" must be set to either 2 or 3 to allow the UFS device to perform DISACRD or ERASE operations when requested from the host. Otherwise, UFS device does not allow the ERASE/DICARD operations. (Refer JESD220D section "12.2.3.1 Erase" and "12.2.3.2 Discard" for more details). From Jdec spec: The erase functionality is implemented using the UNMAP command and it is enabled if the bProvisioningType parameter in the Unit Descriptor is set to 03h (TPRZ = 1). The discard functionality is implemented using the UNMAP command and it is enabled if the 4409 bProvisioningType parameter in the Unit Descriptor is set to 02h (TPRZ = 0). NVIDIA SCL Micron devices came with default value of "0" for the value of bProvisioningType setting. **How does it impact the customer?** UFS memory is erased when provisioned. **If there is a workaround, what is it?** This is the recommended setting for bProvisioningType. **When can we expect the fix?** This is not a bug but a recommended setting for bProvisioningType. **Is it for SDK/PDK?** All
3896611	Kernel	Build kernel from source in SDK and PDK pkg - (Kernel-5.15) Linux
3894016	System Software	**What is the issue?** When flashing with the SDKManager option to "Force wipe of user logins in persistent partition", while the primary user account gets set up correctly, after the system boots the oem-config does not prompt to add more user accounts or enable the secure login feature (i.e. security enhanced SSHD profile). **How does it impact the customer?** You dol not get the option to add more users or enable the secure user login feature (i.e., security enhanced SSHD profile). However, both operations can be done by users logging into the primary user account set up by SDK Manager. **If there is a workaround, what is it?** After SDK Manager flashing is completed, let the system reach the command-line

		prompt, log in to the user account provided in the SDK Manager installation, and run the steps in the SDK documentation sections below. To enable the secure login feature (i.e., security-enhanced SSHD profile), refer the steps in the Install/Update SSH Server section in the Host/Target Setup and Configuration chapter in the *NVIDIA DRIVE OS Linux SDK Developer Guide*. To add more user accounts, refer to the Steps to Change the Username and Password section under the Host/Target Setup and Configuration chapter in the *NVIDIA DRIVE OS Linux SDK Developer Guide*. **When can we expect the fix?** 6.0.8 **Is it for SDK/PDK?** All
3932675	Camera Core	"NOTIF_ERROR_ISP_PROCESSING_FAILURE" pipeline errors and memfault observed when using "IMX728_FPDLINK_RGGB_CPHY_x2" platform configuration
3941557	Graphics	**What is the issue?** Splash screen does not come up on bootup of DRIVE Linux. **How does it impact the customer?** Splash screen will not appear on displays connected to the target. **If there is a workaround, what is it?** N/A **When can we expect the fix?** 6.0.6.1
3892633	Kernel	Reproduce the tegra-ivc panic issue when do the warm reboot stress test

3929506	System Software	**What is the issue?**
		Using depmod -a and then running modprobe does not run for nvme modules due to issues with nvme.ko, nvme-core.ko in /lib/modules/<kernel-version>/updates/dkms/
		How does it impact the customer?
		Without autoloading the modules, the NVME storage does not get detected in DRIVE platform.
		If there is a workaround, what is it?
		Manually load the kernel modules with the commands below after which NVMe devices should get detected and be available for use:
		`$ sudo insmod /lib/modules/5.10.120-rt70-tegra/kernel/drivers/nvme/host/nvme-core.ko`
		`$ sudo insmod /lib/modules/5.10.120-rt70-tegra/kernel/drivers/nvme/host/nvme.ko`
		When can we expect the fix?
		6.0.7
		Is it for SDK/PDK?
		All

3933195	DRIVE Update	Error message seen on update VM: [dulink_remote_ops.c:dulinkRemoteSendWrite:1731]Error 0x2100004 on waitForReply from /auth
3845534	DRIVE Update	Error messages seen intermittently in DRIVE UpdateVM on boot.

3957257	System Software	driveos-oobe-desktop-ubuntu-20.04-rfs.MANIFEST.json is not present on target when flashed with SDKM
3955858	Power Management	Tegra fails to enter SC7 in second cycle
3826383	Connectivity	**What is the issue?** If you do not have the cable connected or incorrect firmware flashed for 88Q4364, then you see the log "Failed to get PCS block lock" for mgbe instance where 88Q4364 PHY is connected. **How does it impact the customer?** Instability in data transfers for mgbe instance where 88Q4364 PHY is connected. For P3710 and P3663, it is the mgbe0 instance. **If there is a workaround/fix, what is it?** 1) Make sure the cable is connected at the line side to have the proper linkup. 2) Flash the latest firmware version 7.1.8.0 provided in SDK/PDK. Firmware and flashing tool paths are listed below: /lib/firmware/marvell_ethernet/88Q4364/ **Firmware update usage:** ./lib/firmware/marvell_ethernet/88Q4364/flash_4364 --install mgbe0_0 Arc-7.1.8.fw.image-ARC_9KB_nvidia_Main_MSMode-GPIO_ID58_VER2031.nvm.bin Once flashed, check the version number: ./lib/firmware/marvell_ethernet/88Q4364/flash_4364 --GetCurrentVersion mgbe0_0 **When can we expect the fix:** N/A **Is it for SDK/PDK?** All
3819124	MCU Firmware	**What is the issue?** On P3663 and 3710 boards with an ES sample of VRS11, VRS11-1 (one of the VRS11) is not accessible for configuration till Tegra boots up as EN signal for this chip is controlled by Tegra and it is only set once Tegra boots up. **How does it impact the customer?** VRS 11 cannot be configured so it results in Read Write mismatch, CRC errors, and HSI latent check failures **If there is a workaround, what is it?** N/A **When can we expect the fix?** This issue gets auto-resolved with the QS sample of VRS11, no SW change is needed. Please contact your VRS-11 device vendor for availability of QS samples. **Is it for SDK/PDK?** All
3679953	MCU Firmware	**What is the issue?** VRS12 may report latent fault due to plausibility check failures during bootup **How does it impact the customer?** There is no functional impact as Tegra is allowed to boot even on failure. However, safety requirements are breached

		If there is a workaround, what is it? Configuring a wider threshold minimizes the occurrence of this fault and this work around is applied in the release 6.0.6 **When can we expect the fix?** Will be fixed in a future release. **Is it for SDK/PDK?** All
3644537	Virtualization	**What is the issue?** Host initiated Refresh (HIR) operation on Micron eMMC device takes around 7 seconds to complete **How does it impact the customer?** If initiated refresh on Micron eMMC from SW, then EMMC becomes busy and no other requests (such as read/write/erase etc.,) are sent to EMMC for that busy period. **If there is a workaround, what is it?** There is no workaround available. Micron is going to provide the eMMC firmware update to reduce the HIR time to 400ms (projected time from Micron). Please check with Micron for more details on this. **When can we expect the fix?** This fix is expected from Micron as an eMMC firmware update. After the new eMMC firmware provided from Micron, it must be flashed to eMMC. For more details, check with Micron. **Is it for SDK/PDK?** All
3738186	Virtualization	Eventlib framework not available in Native Servers.
3769858	Display	Assert observed when display driver kernel modules are loaded
3793667	Camera	**What is the issue?** When isGroupInitProg flag in DeviceBlockInfo structure is set, the links must be initialized in incremental order. **How does it impact the customer?** If the link order is not incremental, some cameras are not initialized correctly so the application cannot receive the frames from the uninitialized cameras. **If there is a workaround, what is it?** The user initializes the cameras in the incremental link order when isGroupInitProg flag is set. **When can we expect the fix?** 6.0.7 **Is it for SDK/PDK?** Linux SDK and PDK.
3803660	Safety Services	**What is the issue?** In 6.0.5.0, there are several known Error IDs reported by FSI during SOC boot up. There errors are: PMRC - CAR_37_UE, CAR_27_UE, CAR_17_UE, CAR_40_UE, CAR_19_UE, CAR_8_UE, PSC - PSC_CLUSTER_UE

		DISPLAY - DISPLAY_UE, DPAUX_0_UE BPMP SW reported errors **How does it impact the customer?** SOC_ERROR pin will be asserted and cannot be de-asserted for the whole power cycle. **If there is a workaround, what is it?** For openbox FSI solution, user can disable above errors in Eps_Cfg.h For closebox FSI solution, the binary has been modified to disable above error during startup, but will re-enable them once it receives the EPS configuration from CCPLEX. User can further disable them for the whole power cycle in the 'SS_ErrorReportingConfig' DT node of Guest OS. **When can we expect the fix?** 6.0.7 **Is it for SDK/PDK?** All
3794297	System Software	Error spews observed in aurix console "ErrorCode-0x89abcdef ReporterId-0x8013"
3794293	MCU Firmware	Error spews observed in aurix console "ErrorCode-0x30000008|ErrorCode-0x2c000008|ErrorCode-0x34000008|ErrorCode-0x38000008 ReporterId-0x8001"
3814954	MCU Firmware	System goes to "power down" or "power off" state upon SC7 entry on INT F1 Board. exitsc7 fails.
3819047	Connectivity	**What is the issue?** "Device initialization is not yet done with status 0x1" error while updating 88Q4364 firmware. **How does it impact the customer?** Unable to update the firmware. **If there is a workaround/fix, what is it?** Firmware should be preflashed in platforms. Before updating the firmware, make sure you read the current version loaded using ./flash_4364 --GetCurrentVersion mgbe0_0. The output should read 7.0.11.0. If any other output is seen, then the firmware is not pre flashed. Contact your NVIDIA support representative for assistance. **When can we expect the fix?** N/A **Is it for SDK/PDK?** All
3819512	System Software	Error spews observed in AURIX console "ErrorCode-0x2a45 ReporterId-0xe02e" after aurixreset.
3819650	Camera	**What is the issue?** nvsipl_camera application auto recovery option might not work properly when multiple cameras are reporting errors. Currently we can only recover the streaming when there is only one camera reporting errors. **How does it impact the customer?** If there are multiple cameras reporting errors, the streaming might not recover for all cameras. The nvsipl_camera will continue to run but some cameras will report

		framerate as 0 fps. **If there is a workaround, what is it?** No workaround for 6.0.6. **When can we expect the fix?** 6.0.7 **Is it for SDK/PDK?** All
3822054	System Software	**What is the issue?** PCIE retimer firmware version 1.13.11 is available, which improves link up. Firmware should be manually update to version 1.13.11. **How does it impact the customer?** P3710-TS4 and TS5 requires 1.13.11 or above. P3710-TS1 through TS3 benefit from 1.13.11 or above. **If there is a workaround, what is it?** Manually update the firmware to version 1.13.11 using the procedure under PCIe Retimer under System Components in the *NVIDIA DRIVE OS 6.0 Linux SDK Developer Guide*. **When can we expect the fix?** Automatic update is planned for upcoming release. **Is it for SDK/PDK** All
3708894	Camera	**What is the issue?** NVIDIA display hardware directly refreshes the output from the image that is bound as input. This means that any changes made to that image buffer will be immediately applied to the display output. This can cause a number of undesirable side effects on the display output, such as tearing or other visual artifacts. In order to avoid these side effects, users should operate using multiple images to interface with the display. In particular, the user should ensure that the currently bound image is never modified. SIPL sample applications that interface with display via OpenWFD, such as nvsipl_camera and nvsipl_sample, currently use a single buffer and hence are susceptible to this type of corruption of the display output. **How does it impact the customer?** Undesirable effects, like tearing or other visual artifacts, may appear on the display output. **If there is a workaround, what is it?** Since this issue is isolated to SIPL sample applications, which are provided in source form, customers can implement their own multi-buffering mechanism (using two or more buffers for interfacing with OpenWFD) to avoid unwanted tearing or other visual artifacts. A reference implementation for such a fix, however, won't be available in DRIVE OS 6.0.6. **When can we expect the fix?** 6.0.7 **Is it for SDK/PDK?** This issue is present in all builds that support interoperation between SIPL and display via a sample application.

3726479	Kernel	**What is the issue?** When USB device is connected, SC7 resume fails. **How does it impact the customer?** If customer is connecting USB device to the board, then SC7 suspend/resume will not work. **If there is a workaround, what is it?** In 6.0.4.0 MCU firmware, after Orin enter SC7 the PREREG power is turned-off by pulling VBAT_SOC_ENA and SOC_PREREG_PWRON pins LOW from the MCU. If suspend-resume cycle is required with USB device the MCU should just put the Orin power regulators in SLEEP mode but should not turn-off the PREREG power. The VBAT_SOC_ENA and SOC_PREREG_PWRON should be driven HIGH from the MCU even when Orin is in SC7 mode. **When can we expect the fix?** Root cause analysis of why USB device is causing resume failure when PREREG is turned-off is still not concluded. Expected fix date will be updated after root-cause analysis. **Is it for SDK/PDK?** All.
3694755	Safety Services	**What is the issue?** In DOS-SHR-5980, HSI T23X-QSPI_HSIv2-3 has not yet been implemented. The HSI expects QSPI errors in PSC to be reported to the Safety Services SW in FSI. **How does it impact the customer?** Customers will not be able to receive QSPI errors in Safety Services SW in FSI. **If there is a workaround, what is it?** Errors are propagated back as return value along the calling sequence to the caller of DRIVE OS API. **When can we expect the fix?** 6.0.7 **Is it for SDK/PDK?** All.
3711131	Camera Core	**What is the issue?** nvsipl_camera application reports error when run with command line option "-plugin 1" The error appears to be during SetExposure call in CDD which sets the new sensor exposure settings computed by auto control algorithm. "--plugin 1" exercises a custom auto control plugin implemented in the sample app and hence may result in different settings than the default auto control algorithm **How does it impact the customer?** If any customer is writing a custom auto control plugin, they may also see the failures. **If there is a workaround, what is it?** No workaround available as the issue is not root caused yet. **When can we expect the fix?** 6.0.7 **Is it for SDK/PDK?**

		All
200775377	System Software	**What is the issue?** PTP client connected to spruce port P7 fails to sync with PTP server due to known bug from Marvell switch firmware. **How does it impact the customer?** Any sensor/device connected to spruce port P7 is not able to sync with PTP server. **If there is a workaround, what is it?** N/A **When can we expect the fix?** The issue is being addressed with the vendor; resolution date is TBD. **Is it for SDK/PDK?** All.
3476824	Docker	**What is the issue?** DRIVE OS support for building and running Docker in Linux Guest OS does not yet support access to the GPU as GPU support is still under study. Docker images can be built and run on the target, but users will not be able to run any GPU-accelerated containers. **How does it impact the customer?** The customer will not be able to run any containerized GPU workloads **If there is a workaround, what is it?** The user must manually include the required devices and mounts in the docker command line using the --device and -v flags. In addition, the user would have to run ldconfig in the container to ensure that the libraries are available in the LD cache **When can we expect the fix?** 6.0.7
3474024	DRIVE Update	**What is the issue?** DRIVE Update fails to switch chain via scratch method. That method is used to verify the newly updated boot chain before permanent switching of bootchain via BR_BCT. While switching boot chain via scratch method, a mb1 reset is observed which is switch the chain back to original chain. This bug can be blocker for SW update if they are using this feature. **How does it impact the customer?** Customer may not be able to validate the newly updated chain before final switch for boot chain. **If there is a workaround, what is it?** There is no WAR for this issue. We are still debugging root cause. Till now it seems p3663 platform specific. **When can we expect the fix?** We are working on root causing this issue.
200618961	System Software	Low frames per second (FPS) observed while replaying LRAW/RAW videos with the Camera Replay Sample.
3937904		**[New Issue]** Camera replay samples not working and failed with error libnvemu_470.141.03.01.so: cannot open shared object file after upgrading the NVIDIA driver to R470.141.03 in the x86 host system.
3925551		**[New Issue]** Sample_camera & recorder-cli tool recorded raw/lraw video playback

3906473		fails
3925474		**[New Issue]** Header dump tool failed for lidar and radar with error: Could not cast to virtual sensor. [TC ID: 41643, 41645]
3929493		**[New Issue]** Video not rendered properly after export from lraw/raw for AR0820, IMX728 Camera. Screen appeared in black color only.
	Image and Point Cloud Processing	The following algorithms are not supported on Orin’s OFA and/or PVA engines in this release: • ImageFilter (Recursive Gaussian Filter, BoxFilter, 2Dconv). • FAST9 Feature Detector, Standard Harris Corner Detector. • IC and fastIC Feature Tracker. • DenseOpticalFlow. • Stereo. • Template Tracker.
3496936		[DW5.2-RC3/6.0.2.0/ORIN] sample_stereo_disparity dumps "Error calling GL deleter" on console.
		Tensor Streaming is not operational in this release.
3754813		Video_exporter fails with error: DW_INVALID_ARGUMENT: calculateImageLayout: plane count 0 and format 0 combination is invalid
3837111		ORB feature detector and descriptor show low performance.
3821840		sample_connected_components with video input (raw/lraw/h264) do not show preview window
3838236		**[New Issue]** sample_image_pyramid_pva failing with DW_INVALID_ARGUMENT: Image Pyramid Task creation failed As a workaround: • Manually install the DW core lib “driveworks_5.10.87~linux6.0.6-323457480_arm64.deb” which updates the “/usr/lib/firmware/pva_auth_allowlist” then reboot in order to make PVA accessible. Verify by checking that the response to command “sha256sum /usr/lib/firmware/pva_auth_allowlist” is “0b8e1c857169250305207c4cb02693e09ac324ffaae959452ccf0171fcb39df7 /usr/lib/firmware/pva_auth_allowlist” • Use --useHalfRes=0 when calling sample_feature_tracker to run with PVA. Call should look like this: "./sample_feature_tracker --pvaPyramid=1 --pvaDetector=1 --pvaTracker=1 --useHalfRes=0"
3931886	DNN Framework	**[New Issue]** DNN samples don’t support Caffe models, detection will not work properly with the default models.
3824086	Calibration	Calibration-recorder tool with raw video input, doesn’t show preview window. (No issue seen with lraw and h264 formats)
3948392	CGF	**[New Issue]** sample_cgf_dwchannel in inter-process nvscistream with asynchronous mode fails, execution stuck
200778230 3598944	General	Nuisance Error Messages that do not affect functionality: • All samples dump error on console: No resources(.pak) mounted from '/usr/local/driveworks-5.0/data'. Please adjust path or some modules won't

		function properly. Recorder-qtgui and recorder-tui fail to launch: ModuleNotFoundError: No module named 'Crypto'.
3946033	STM	**[New Issue]** The STM manual is not included in the release package. For NVONLINE users, it will be posted as a separated .zip file. The docs will also be uploaded to DevZone for DevZone and NGC users.
200778085	SAL	Video Exporter Tool fails.
3408375		SIPL recorded playback of 16 8MP raw/lraw video failed.
200782352		LRAW Preview Extraction Tool fails.
2539131		Xsens has a reordering issue with timestamps when reset.
3602138		Initialize/release dwFrameCapture in loop will lead system run out of memory.
3494734		**What is the issue?** Some networks may suffer accuracy degradation when run on DLA with large batch sizes. **How does it impact the customer?** When running networks on DLA with batch sizes larger than 32, accuracy may degrade. **If there is a workaround, what is it?** To work around this issue, use a smaller batch size. **When can we expect the fix?** The issue will be fixed in a future DLA release. **Is it for SDK/PDK?** Safety, SDK
3498326		**What is the issue?** There is a known issue with DLA clocks that requires users to reboot the system after changing the nvpmodel power mode or otherwise experience a performance drop. **How does it impact the customer?** Performance may drop significantly after changing the nvpmodel power mode. **If there is a workaround, what is it?** Reboot the system after changing the nvpmodel power mode. **When can we expect the fix?** 6.0.7 **Is it for SDK/PDK?** Safety, SDK

Release Properties

The following table describes the release properties and software versions.

Release Properties	
Property	**Description**
Linux	Specifies the operating system.
20.04	Specifies the host Ubuntu operating system version.
Focal Fossa	Specifies the codename for the host version of Ubuntu.
20.04	Specifies the target root file system operating system version.
6.0.6	Specifies the NVIDIA release branch number.
32443318	Specifies the build ID for the Linux operating system.
32441545	Specifies the build ID for the Linux Knext operating system.
drive-linux	Specifies the product name.
Linux	Specifies the platform.
234	Specifies the architecture version.
Software Version	
Software	**Version**
GCC Cross-compiler Toolchain for user applications and libraries for Yocto root file system.	9.3
GCC Cross-compiler Toolchain for user applications and libraries for Ubuntu root file system.	9.3
OpenGL ES	3.2
OpenGL: Provided for development purposes. Production systems are expected to use OpenGL ES.	4.6
Wayland	1.18
Vulkan Provided for development purposes. Safety systems are expected to use Vulkan SC.	1.3

Vulkan SC	1.0
OpenWF Display	1.0
DriveWorks	5.10
DLA	3.12[1]
CUDA	11.4.20
cuDNN	8.6.0
TensorRT	8.5.10
ONNX	1.9.0 and opset 13
TensorFlow	1.15.0
PyTorch	1.9.0
Elementwise	2.4.2

DRIVE OS Supported Sensors

For a list of supported sensors, see the Supported Sensors chapter under Setup and Configuration section in the *NVIDIA DRIVE OS Linux Developer Guide*.

CUDA

The following table describes CUDA support.

Host OS	Host OS Version	Target OS	Target OS Version	Compiler Support
Ubuntu	20.04 LTS	Ubuntu	Ubuntu 20.04	GCC 9.3

Standard

The current release label is 11.4.20. The various components in the toolkit are versioned independently. The following table shows each component and its version:

Component Name	Version Information	Supported Architectures
CUDA Runtime (cudart)	11.4.327	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
cuobjdump	11.4. 327	Linux (aarch64), Linux (x86_64)
CUPTI	11.4. 327	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64

[1] DLA versions 1.3.7, 1.3.8, 3.9.0, and 3.10 are also supported.

CUDA cuxxfilt (demangler)	11.4. 327	Linux (aarch64), Linux (x86_64)
CUDA Demo Suite	11.4. 327	Linux (x86_64)
CUDA GDB	11.4. 327	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA NVCC	11.4. 327	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA nvdisasm	11.4. 327	Linux (aarch64), Linux (x86_64)
CUDA NVML Headers	11.4. 327	Linux (aarch64), Linux (x86_64)
CUDA nvprof	11.4. 327	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA nvprune	11.4. 327	Linux (aarch64), Linux (x86_64)
CUDA NVRTC	11.4. 327	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA NVTX	11.4. 327	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA NVVP	11.4. 327	Linux (x86_64)
CUDA Samples	11.4. 327	l4t_aarch64, Linux (aarch64), Linux (x86_64)
CUDA Compute Sanitizer API	11.4. 327	Linux (aarch64), Linux (x86_64)
CUDA Thrust	11.4. 327	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA cuBLAS	11.6.6.111	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA cuDLA	11.4. 327	Linux (aarch64), qnx-standard_aarch64
CUDA cuFFT	10.6.0.231	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA cuRAND	10.2.5.326	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA cuSOLVER	11.2.0.326	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA cuSPARSE	11.6.0.326	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA NPP	11.4.0.316	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
Nsight Compute	2021.2.8.1	Linux (x86_64), qnx-standard_aarch64
Nsight Systems	2022.4.2.23	Linux (x86_64)
NVIDIA Linux Driver	470.161.03	Linux (x86_64)

Notice

The information provided in this specification is believed to be accurate and reliable as of the date provided. However, NVIDIA Corporation ("NVIDIA") does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This publication supersedes and replaces all other specifications for the product that may have been previously supplied.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and other changes to this specification, at any time and/or to discontinue any product or service without notice. Customer should obtain the latest relevant specification before placing orders and should verify that such information is current and complete.

NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer. NVIDIA hereby expressly objects to applying any customer general terms and conditions with regards to the purchase of the NVIDIA product referenced in this specification.

NVIDIA products are not designed, authorized or warranted to be suitable for use in medical, military, aircraft, space or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer's own risk.

NVIDIA makes no representation or warranty that products based on these specifications will be suitable for any specified use without further testing or modification. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer's sole responsibility to ensure the product is suitable and fit for the application planned by customer and to do the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer's product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this specification. NVIDIA does not accept any liability related to any default, damage, costs or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this specification, or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this specification. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA. Reproduction of information in this specification is permissible only if reproduction is approved by NVIDIA in writing, is reproduced without alteration, and is accompanied by all associated conditions, limitations, and notices.

ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, "MATERIALS") ARE BEING PROVIDED "AS IS." NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA's aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the NVIDIA terms and conditions of sale for the product.

VESA DisplayPort

DisplayPort and DisplayPort Compliance Logo, DisplayPort Compliance Logo for Dual-mode Sources, and DisplayPort Compliance Logo for Active Cables are trademarks owned by the Video Electronics Standards Association in the United States and other countries.

HDMI

HDMI, the HDMI logo, and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing LLC.

OpenCL

OpenCL is a trademark of Apple Inc. used under license to the Khronos Group Inc.

Blackberry

BLACKBERRY, EMBLEM Design, QNX, AVIAGE, MOMENTICS, NEUTRINO and QNX CAR are the trademarks or registered trademarks of BlackBerry Limited, used under license, and the exclusive rights to such trademarks are expressly reserved.

Trademarks

NVIDIA and the NVIDIA logo are trademarks and/or registered trademarks of NVIDIA Corporation in the U.S. and other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

Copyright