NVIDIA DRIVE OS 6.0.7 Linux

Release Notes

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 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.

Deprecations in this Release

The following items are deprecated in this release:

Summary	Module	Impact
Application call-back functions are statically configured through the configurator. The following APIs were removed: • DMA_register_callback() • DMA_register_callback_param() • DMA_deregister_callback() • DMA_deregister_callback_param()	DMA CDD	• Applications can no longer call these APIs to register/un-register application call-backs. • Applications must remove calls to these APIs. • Call-back functions need to be statically configured through the DMA CDD configuration tool provided by the AUTOSAR vendor.
Removal of the redundant/unused APIs: • DMA_Channel_Update() • DMA_Update_Fixed_Pattern_Transfer()	DMA CDD	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 are no longer able to change DMA channel configuration at run-time i.e., all DMA channels are configured statically. • DMA_Update_Fixed_Pattern_Transfer() • Applications must remove calls to this API, if used. This API is expected to be unused.
Key-on and key-off support in the same boot cycle has been removed.	Standard	You can still choose to run KIST at KeyOn or KeyOff via the MCU and what you choose executes the same test. Only one KIST result is stored; therefore, results must be checked between each KIST run to avoid losing the result.

The DeviceBlockInfo isSimulatorModeFlag flag has been deprecated. The isSimulatorModeFlag has been added to the CameraModuleInfoList structure.	Standard	There is no impact if you do not develop sample applications. If you do, use CameraModuleInfoList isSimulatorModeFlag.
NvMediaIJPESetNvSciSyncObjforSOF, NvMediaIJPEGetSOFNvSciSyncFence, NvMediaIJPDGetSOFNvSciSyncFence, NvMediaIJPDSetNvSciSyncObjforSOF APIs are deprecated in 6.0.7.0.	Standard	Discontinue use of these API.
NvMediaEncodeQuality and enableNewPreset have been removed.	NvMedia	NvMediaEncodeQuality enumeration has been deprecated and the enableNewPreset Boolean used to switch between old and new API has been removed. Move to NvMediaEncPreset enumerations.
camRecCfg variable has been deprecated.	Standard	The camRecCfg variable, located in struct DeserInfo in NvSIPLDeviceBlockInfo.hpp file, is now deprecated. Applications with this variable configured must remove this variable.

Planned Upcoming Changes

The following sections describe planned, upcoming changes.

Summary	Module	Impact
The SiplControlISPStatsSetting structure defined in NvSiplControlAutoDef.hpp will be deprecated in 6.0.8.	Standard and Safety	No impact.
The const keyword will be removed in the API below in 6.0.8: ```NvMediaStatus NvMediaIDERegisterNvSciBufObj (const NvMediaIDE *decoder, //May be used in future to pin the surface NvSciBufObj bufObj```	NvMedia	This will be modified to: ```NvMediaStatus NvMediaIDERegisterNvSciBufObj (NvMediaIDE *decoder, //May be used in future to pin the surface NvSciBufObj bufObj``` This does not deprecate the API or modify any of the existing fields/parameters.

NvMediaIJPEGetBitsEx APIs is planned to be deprecated in 6.0.8.0.	Standard	Discontinue use of this API and initiate the transition to alternate API.
6.0.8 will remove public debug API NvMediaIOFAGetProfileData from all builds and OSes and remove the NvMediaIofaProfileMode argument from the NvMediaIofaInitParams structure as it was getting used by NvMediaIOFAGetProfileData.	Standard	NvMediaIOFAGetProfileData API is not used in production for perf measurement. nvm_iofa_flow_sci and nvm_iofa_stereo_sci have now moved to NvPlayFair APIs for perf measurement and NvMediaIOFAGetProfileData is not used for getting perf numbers.

New Features and Enhancements

This release includes support for these new features and enhancements.

New Features for DRIVE OS

FSI Boot and Functionality in Absence of FSI Keys in Secure Storage

DRIVE OS supports FSI boot and functionality in absence of FSI keys in secure storage.

Support for Removable NVMe Storage (Linux PDK)

DRIVE OS supports Guest VM to perform read/write transactions from NVMe storage devices directly connected to Orin PCIe Gen4 controller via x4 PCIe lanes. When DRIVE OS transitions from suspend to resume state, the read/write operation to NvMe device continues to be fully functional in the same way it was prior to the suspend state. The NVMe storage device must be from the NVIDIA Orin Supported Component List.

Orin SoC HSI (SW Enabled HW Faults – Non-Safety Products)

DRIVE OS provides HW fault reporting services for the I/Ps where fault signals are not routed to HSM. The software driver of corresponding I/Ps on CCPLEX detect the fault and propagate to FSI. FSI has have capability to propagate these errors to MCU.

PKCS#11 Support for Key Derivation

DRIVE OS implements the following PKCS #11 cryptographic mechanisms [PKCS11-CURR-v3.0] with the listed PKCS#11 functions [PKCS11-BASE-v3.0] using the Hardware Security Offload Engine hardware:

PKCS#11 Functions	PKCS#11 Mechanisms	Key Sizes
C_DeriveKey	CKM_SP800_108_COUNTER_KDF	• 128 bits • 256 bits
	CKM_NVIDIA_SP800_56C_TWO_STEPS_KDF	• 128 bits • 256 bits
	CKM_TLS12_MASTER_KEY_DERIVE_DH	• 384 bits
	CKM_TLS12_KEY_AND_MAC_DERIVE	• 128 bits • 256 bits
	CKM_TLS12_KEY_SAFE_DERIVE	• 128 bits • 256 bits
	CKM_TLS12_KDF	• 128 bits • 256 bits

DRIVE Orin Nano (P3898)

DRIVE OS supports DRIVE Orin Nano reference design (P3898 SKU0 TS1) for L2 ADAS.

Enable Radial Lens Shading

DRIVE OS provides a mechanism to add calibration data for Radial LSC parameters to enable the Radial Lens Shading HW subunit. DRIVE OS loads Sensor and ISP specific calibration data from the user provided memory blob at initialization time.

UFS Stream ID

To address a security feature, starting in 6.0.7.0, every virtualized UFS partition must be configured with a stream ID.

In storage configuration, all virtualized UFS partitions must be configured with the ufs_stream_id attribute, or the system may crash or may not boot.

The UFS stream ID does not have to be unique for Linux.

For the configuration procedure, refer to the documentation located under AV PCT Configuration at Configuring the UFS Stream ID for Virtualized UFS Partitions in the *NVIDIA DRIVE OS 6.0 Developer Guide*.

SoC Error Pin

There is an update in SOC error pin toggling frequency and the SOC error pin assertion detection mechanism in 6.0.7.0. The SOC error pin assertion detection mechanism on MCU has been updated to use a periodic OS task instead of using the GTM hardware module on MCU. Due to concerns of mixed ASIL software (customer software and DRIVE OS) using the GTM module, DRIVE OS ASIL-D software cannot use GTM. The SOC error pin toggling period is updated on Orin. The SOC error pin assertion

detection mechanism is updated on the MCU to comply with the update in SOC error pin toggling period on Orin.

Ensure that the 6.0.7.0 DRIVE OS SDK and PDK release (FSI Firmware 1.6.x) is flashed on Orin and the latest 6.0.7.0 MCU firmware (5.10.xx AFW) is flashed on AURIX MCU. Older releases are not compatible with 6.0.7.0 MCU firmware (5.10.xx AFW). MCU firmware of older releases are not compatible with 6.0.7.0 (FSI firmware 1.6.x).

Build-FS and Copytarget Workflow

Due to the kernel version being a variable of a component outside of Build-FS and copytarget, if Build-FS or copytarget directly or indirectly must copy kernel modules, then the following shell variables must be set before running copytarget and Build-FS:

```
export PROD_SUFFIX=<str> # where <str> is "" (empty ) if using standard
kernel and is "_prod" if using production kernel modules.
export NVRTKERNELNAME="$(basename $NV_WORKSPACE/drive-
linux/kernel/preempt_rt${PROD_SUFFIX}/modules/rt-tegra)"
```

QM Storage Server

To mitigate possible violation of availability requirements of an application due to QM storage server, the following measures have been added:

- Reduce priority of storage server and make it the same as GOS VM.
- Reduce time slice of storage server and GOS VM and set it to 40 us each.

NvSciSync: Profiling Support with Nsight Systems

Profiling of task submission and execution on VPU via Nsight systems is now supported. You can profile the workloads submitted to the PVA.

4GB Buffer Allocation Support

Allocation of buffers and importing buffers larger than 4GB is now allowed across the PVA stack. You can use larger buffers for workloads submitted to the PVA.

PVA Performance Improvements

PVA Command launch time is now significantly improved.

New Features for DriveWorks 5.12

This release includes support for these new features and enhancements.

New Features and Improvements

- Introduce cuDLA API for DNN framework, accessible via sample_dnn_tensor, refer to the *DriveWorks SDK Reference*. This enables developers to run workloads on DLA via the DNN framework.
- Support for Smartlead IMX 623 B2 and IMX 728 B2.

Installation and Getting Started

- DriveWorks 5.12 is installed with DRIVE OS 6.0.7.0. 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
3558625	IST	**What was the issue?** The Key On IST test sometimes failed the first execution after flashing a new build on Orin. Subsequent tests were expected to pass. **How did it impact the customer?** The first Key On IST run after flashing might have failed. **Was it for SDK/PDK?** All
3819124	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 the configuration until Tegra booted up, as EN signal for this chip was controlled by Tegra and it was only set once Tegra booted up. **How did it impact the customer?** VRS 11 could not be configured so it resulted in Read Write mismatch, CRC errors, and HSI latent check failures. **Was it for SDK/PDK?** All
3476824	Docker	**What was the issue?** DRIVE OS support for building and running Docker in Linux Guest OS did not yet support access to the GPU as GPU support was still under study. Docker images could be built and ran on the target, but users were not able to run any GPU-accelerated containers. **How did it impact the customer?** The customer was not able to run any containerized GPU workloads.
3803660	Safety Services	**What was the issue?** In 6.0.5.0, there were several known Error IDs reported by FSI during SOC boot up. There errors were: 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 did it impact the customer? SOC_ERROR pin was asserted and could not be de-asserted for the whole power cycle. **Was it for SDK/PDK?** All
3946033	STM	The STM manual was not included in the release package. For NVONLINE users, it was posted as a separated .zip file. The docs were also uploaded to DevZone for DevZone and NGC users.
3839935	IST	**What was the issue?** Some systems failed KIST. **How did it impact the customer?** You might have seen false KIST failures on some systems. **Was it for SDK/PDK?** PDK
3819047	Connectivity	**What was the issue?** "Device initialization is not yet done with status 0x1" error while updating 88Q4364 firmware. **How did it impact the customer?** Unable to update the firmware. **Was it for SDK/PDK?** All
3819512	System Software	Error spews observed in AURIX console "ErrorCode-0x2a45 ReporterId-0xe02e" after aurixreset.
3929506	System Software	**What was the issue?** Using depmod -a and then running modprobe did not run for nvme modules due to issues with nvme.ko, nvme-core.ko in /lib/modules/<kernel-version>/updates/dkms/. **How did it impact the customer?** Without autoloading the modules, the NVME storage did not get detected in DRIVE platform. **Was it for SDK/PDK?** All
3751073	System Software	**What was the issue?** Hardware limitation (PMIC and Board design) where an older revision of P3663 and P3710 could not support SC7. **How did it impact the customer?** You could not use an older revision of the board for SC7 testing. **Was it for SDK/PDK?** All
3814954	MCU	System went to "power down" or "power off" state upon SC7 entry on INT F1

	Firmware	Board. exitsc7 failed.
3794297	System Software	Error spews observed in aurix console "ErrorCode-0x89abcdef ReporterId-0x8013"
3822054	System Software	**What was the issue?** PCIE retimer firmware version 1.13.11 was available, which improved link up. Firmware should have been manually updated to version 1.13.11. **How did it impact the customer?** P3710-TS4 and TS5 required 1.13.11 or above. P3710-TS1 through TS3 benefited from 1.13.11 or above. **Is it for SDK/PDK** Both
3955858	Power Management	Tegra failed to enter SC7 in second cycle.
3738186	Virtualization	Eventlib framework was not available in Native Servers.
200778085	SAL	Video Exporter Tool failed.
3474024	DRIVE Update	**What was the issue?** DRIVE Update failed to switch chain via scratch method. That method was used to verify the newly updated boot chain before permanent switching of bootchain via BR_BCT. **How did it impact the customer?** You might not have been able to validate the newly updated chain before final switch for boot chain.
3952902	IST	**What was the issue?** KIST reported failure with Linux Kernel 5.15. **How did it impact the customer?** You could not use KIST with 5.15 kernel (kernel-5.10 was working). **Was it for SDK/PDK?** PDK
3892633	Kernel	Reproduced the tegra-ivc panic issue when doing the warm reboot stress test.
3896611	Kernel	Built kernel from source in SDK and PDK pkg - (Kernel-5.15) Linux
3726479	Kernel	**What was the issue?** When USB device was connected, SC7 resume failed. **How did it impact the customer?** If you were connecting USB device to the board, then SC7 suspend/resume did not work. **Was it for SDK/PDK?** All.
3957257	System Software	**What was the issue?** Due to build-FS tool issues, the SDKM update process done by Build-FS to set up the user account removed the filesystem manifest information (and also the manifest filename that indicated the variant of the filesystem). **How did it impact the customer?** After SDKM installation, if you checked the directory

		/etc/nvidia/rootfilesystem-manifest, you saw the following files:

ID	Component	Description
		/etc/nvidia/rootfilesystem-manifest, you saw the following files: • tmp.MANIFEST.json • driveos-rfs.MANIFEST.json (symlink pointing to tmp.MANIFEST.json) Without SDK installed (which was in pre-flash boards) the user checking the directory /etc/nvidia/rootfilesystem-manifest saw 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) **Was it for SDK/PDK?** All
3894016	System Software	**What was 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 did not prompt to add more user accounts or enable the secure login feature (i.e., security enhanced SSHD profile). **How did it impact the customer?** You did not get the option to add more users or enable the secure user login feature (i.e., security enhanced SSHD profile). However, both operations could be done by users logging into the primary user account set up by SDK Manager. **Was it for SDK/PDK?** All
3794293	MCU Firmware	Error spews observed in aurix console "ErrorCode-0x30000008|ErrorCode-0x2c000008|ErrorCode-0x34000008|ErrorCode-0x38000008 ReporterId-0x8001"
3837369	Safety MCU Firmware	**What was the issue?** MCU software hung due to I2C transactions during IST. **How did it impact the customer?** Board hung during AURIX bootup. **Was it for SDK/PDK?** All
3679953	MCU Firmware	**What was the issue?** VRS12 might have reported latent fault due to plausibility check failures during bootup **How did it impact the customer?** There was no functional impact as Tegra was allowed to boot even on failure. However, safety requirements were breached. **Was it for SDK/PDK?** All
3941557	Graphics	**What was the issue?** Splash screen did not come up on bootup of DRIVE Linux. **How did it impact the customer?** Splash screen did not appear on displays connected to the target.
3602138	SAL	Initialize/release dwFrameCapture in loop led the system to run out of

		memory.
3826383	Connectivity	**What was the issue?** If you did not have the cable connected or incorrect firmware flashed for 88Q4364, then you saw the log "Failed to get PCS block lock" for mgbe instance where 88Q4364 PHY was connected. **How did it impact the customer?** Instability in data transfers for mgbe instance where 88Q4364 PHY was connected. For P3710 and P3663, it was the mgbe0 instance. **Was it for SDK/PDK?** All
3932675	Camera Core	**What was the issue?** The SIPL camera sample applications Serializer (TI DS90UB971) TPG configurations (DS90UB971_RAW12_TPG_CPHY_x4 and DS90UB971_RAW12_TPG_DPHY_x4) failed to initialize and began streaming on QNX. **How did it impact the customer?** Unable to use the DS90UB971_RAW12_TPG_CPHY_x4 and DS90UB971_RAW12_TPG_DPHY_x4 Serializer (TI DS90UB971) TPG configurations in SIPL camera sample applications. **Was it for SDK/PDK?** TI FPD-Link support was only present in the standard build, the configuration is present in the SDK and PDK.
3819650	Camera	**What was the issue?** nvsipl_camera application auto recovery option might not have worked properly when multiple cameras were reporting errors. You could only recover the streaming when there was only one camera reporting errors. **How did it impact the customer?** If there were multiple cameras reporting errors, the streaming might not have recovered for all cameras. The nvsipl_camera would continue to run but some cameras would report the framerate as 0 fps. **Was it for SDK/PDK?** All
3852875	Camera	**What was the issue?** The PDK source build broke due to the migration of the NvMedia core header to a 6.x version. **How did it impact the customer?** You were unable to build camera device drivers from source. **Was it for SDK/PDK?** All
3830784	Camera	**What was the issue?** In Reprocess mode, the timestamps - frameCaptureTSC and frameCaptureStartTSC that could be optionally provided as inputs to NvSIPLImageGroupWriter::RawBuffer struct showed up swapped as frameCaptureStartTSC and frameCaptureTSC when read from corresponding fields of INvSIPLClient::ImageMetaData from the output buffer.

		How did it impact the customer?
		In reprocess mode you were not able to see the programmed SOF and EOF timestamps properly in the output buffer metadata.
		Was it for SDK/PDK?
		All
3708894	Camera	**What was the issue?**
		NVIDIA display hardware directly refreshed the output from the image that was bound as input. This meant that any changes made to that image buffer were immediately applied to the display output. This caused a number of undesirable side effects on the display output, such as tearing or other visual artifacts.
		SIPL sample applications that interface with display via OpenWFD, such as nvsipl_camera and nvsipl_sample, used a single buffer and hence were susceptible to this type of corruption of the display output.
		How did it impact the customer?
		Undesirable effects, like tearing or other visual artifacts, may have appeared on the display output.
		Was it for SDK/PDK?
		This issue was present in all builds that supported interoperation between SIPL and display via a sample application.
3711131	Camera Core	**What was the issue?**
		nvsipl_camera application reported error when ran with command line option "-plugin 1"
		The error appeared to be during SetExposure call in CDD, which set the new sensor exposure settings computed by auto control algorithm.
		"--plugin 1" exercised a custom auto control plugin implemented in the sample app and hence may have resulted in different settings than the default auto control algorithm
		How did it impact the customer?
		If you were writing a custom auto control plugin, you may have seen the failures.
		Was it for SDK/PDK?
		All
4041239	Security	**What was the issue?**
		Prior to release 6.0.7.0, the PKCS#11 Library mistakenly expected the mechanism CKM_SHAXXX_RSA_PKCS_PSS in the hashAlg field of CK_RSA_PKCS_PSS_PARAMS rather than the actual digest mechanism CKM_SHAXXX.
		How did it impact the customer?
		The wanted digest mechanism CKM_SHAXXX was rejected.
		Applies to: Standard and Safety, SDK and PDK.
3694755	Safety Services	**What was the issue?**
		In DOS-SHR-5980, HSI T23X-QSPI_HSIv2-3 had not yet been implemented. The HSI expected QSPI errors in PSC to be reported to the Safety Services SW in FSI.
		How did it impact the customer?

		You were not able to receive QSPI errors in Safety Services SW in FSI. **Was it for SDK/PDK?** All.
3845534	DRIVE Update	Error messages seen intermittently in DRIVE Update VM on boot.
3974700	Video	Support for YUV444 lossy encoding was not possible in earlier releases and is now supported.
3408375	SAL	SIPL recorded playback of 16 8MP raw/lraw video failed.
3937904		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 3906473		Sample_camera & recorder-cli tool recorded raw/lraw video playback fails
2539131		Xsens has a reordering issue with timestamps when reset.
3754813	Image and Point Cloud Processing	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.
3838236		sample_image_pyramid_pva failing with DW_INVALID_ARGUMENT: Image Pyramid Task creation failed
3821840		sample_connected_components with video input (raw/lraw/h264) do not show preview window
3931886	DNN Framework	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, does't show preview window. (No issue seen with lraw and h264 formats)
3948392	CGF	sample_cgf_dwchannel in inter-process nvscistream with asynchronous mode fails, execution stuck
200778230	General	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*
3598944		Recorder-qtgui and recorder-tui fail to launch: ModuleNotFoundError: No module named 'Crypto'.

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
CVE-2022-2588	3781441	A use-after-free flaw was found in route4_change in the net/sched/cls_route.c filter implementation in the Linux kernel. This flaw allows a local, privileged

		attacker to crash the system, possibly leading to a local privilege escalation issue.
CVE-2022-2318	3781569	NVIDIA distributions of Linux contains a use-after-free vulnerability in timer handler in net/rose/rose_timer.c, where an 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-2022-29582	3783109	In the Linux kernel before 5.17.3, fs/io_uring.c has a use-after-free due to a race condition in io_uring timeouts. This can be triggered by a local user who has no access to any user namespace; however, the race condition perhaps can only be exploited infrequently.
CVE-2022-20399	3783109	In the SEPolicy configuration of system apps, there is a possible access to the 'ip' utility due to an insecure default value. This could lead to local information disclosure of network data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-219808546References: Upstream kernel"
CVE-2022-2503	3785692	Dm-verity is used for extending root-of-trust to root filesystems. LoadPin builds on this property to restrict module/firmware loads to just the trusted root filesystem. Device-mapper table reloads currently allow users with root privileges to switch out the target with an equivalent dm-linear target and bypass verification till reboot. This allows root to bypass LoadPin and can be used to load untrusted and unverified kernel modules and firmware, which implies arbitrary kernel execution and persistence for peripherals that do not verify firmware updates. We recommend upgrading past commit 4caae58406f8ceb741603eee460d79bacca9b1b5
CVE-2022-36946	3785692	nfqnl_mangle in net/netfilter/nfnetlink_queue.c in the Linux kernel through 5.18.14 allows remote attackers to cause a denial of service (panic) because, in the case of an nf_queue verdict with a one-byte nfta_payload attribute, an skb_pull can encounter a negative skb->len.
CVE-2022-36879	3785692	An issue was discovered in the Linux kernel through 5.18.14. xfrm_expand_policies in net/xfrm/xfrm_policy.c can cause a refcount to be dropped twice.

CVE-2021-33656	3785692	When setting font with malicous data by ioctl cmd PIO_FONT,kernel will write memory out of bounds.
CVE-2022-2380	3785692	The Linux kernel was found vulnerable out of bounds memory access in the drivers/video/fbdev/sm712fb.c:smtcfb_read() function. The vulnerability could result in local attackers being able to crash the kernel.
CVE-2022-32250	3785692	net/netfilter/nf_tables_api.c in the Linux kernel through 5.18.1 allows a local user (able to create user/net namespaces) to escalate privileges to root because an incorrect NFT_STATEFUL_EXPR check leads to a use-after-free.
CVE-2022-20409	3814890	In io_identity_cow of io_uring.c, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-238177383References: Upstream kernel.
CVE-2022-20422	3814890	In emulation_proc_handler of armv8_deprecated.c, there is a possible way to corrupt memory due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-237540956References: Upstream kernel.
CVE-2023-20928	3924637	In binder_vma_close of binder.c, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254837884References: Upstream kernel.
CVE-2022-42721	3924637	A list management bug in BSS handling in the mac80211 stack in the Linux kernel 5.1 through 5.19.x before 5.19.16 could be used by local attackers (able to inject WLAN frames) to corrupt a linked list and, in turn, potentially execute code.
CVE-2022-42719	3924637	A use-after-free in the mac80211 stack when parsing a multi-BSSID element in the Linux kernel 5.2 through 5.19.x before 5.19.16 could be used by attackers (able to inject WLAN frames) to crash the kernel and

		potentially execute code.
CVE-2022-42720	3924637	Various refcounting bugs in the multi-BSS handling in the mac80211 stack in the Linux kernel 5.1 through 5.19.x before 5.19.16 could be used by local attackers (able to inject WLAN frames) to trigger use-after-free conditions to potentially execute code.
CVE-2022-41674	3924637	An issue was discovered in the Linux kernel before 5.19.16. Attackers able to inject WLAN frames could cause a buffer overflow in the ieee80211_bss_info_update function in net/mac80211/scan.c.
CVE-2021-33655	3924637	When sending malicous data to kernel by ioctl cmd FBIOPUT_VSCREENINFO,kernel will write memory out of bounds.
CVE-2022-41222	3925462	mm/mremap.c in the Linux kernel before 5.13.3 has a use-after-free via a stale TLB because an rmap lock is not held during a PUD move.
CVE-2022-39842	3925462	** DISPUTED ** An issue was discovered in the Linux kernel before 5.19. In pxa3xx_gcu_write in drivers/video/fbdev/pxa3xx-gcu.c, the count parameter has a type conflict of size_t versus int, causing an integer overflow and bypassing the size check. After that, because it is used as the third argument to copy_from_user(), a heap overflow may occur. NOTE: the original discoverer disputes that the overflow can actually happen.
CVE-2022-39189	3925462	An issue was discovered the x86 KVM subsystem in the Linux kernel before 5.18.17. Unprivileged guest users can compromise the guest kernel because TLB flush operations are mishandled in certain KVM_VCPU_PREEMPTED situations.
CVE-2022-43680	3937457	In libexpat through 2.4.9, there is a use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate in out-of-memory situations.

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
3972843	System software	CUB is experimental on Tegra products.

Known Issues

<table>
<tr><td>**Note:**</td><td>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*.</td></tr>
</table>

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

Feature	Module	Description
3961157	Camera Core	**What is the issue?** Demosaic of RGB-IR sensors in nvsipl_camera is not supported. When `--enableRawOutput` is used with Display in nvsipl_camera, the app fails. **How does it impact the customer?** You cannot display raw output of RGB-IR sensors. **If there is a workaround, what is it?** N/A **When can we expect the fix?** 6.0.8 Note: A demosaic'd image will not be displayed; a monochrome image created using G and IR components will be displayed. **Is it for SDK/PDK?** Both
4087839	System Software	**What is the issue?** In bind phase of the build, storage configuration may throw the warning message: "WARNING: Uniqueness failure: Reuse of SID value:". **How does it impact the customer?** The Warning "WARNING: Uniqueness failure: Reuse of SID value:" can be ignored for Linux and boot chain C builds. **If there is a workaround, what is it?** N/A **When can we expect the fix?** 6.0.8 **Is it for SDK/PDK?** Both
4079505	Filesystem	**What is the issue?**

The kernel K5.10 builds many of the loadable kernel modules (*.ko), and all kernel modules are copied to the filesystem regardless of whether they are used. This is suboptimal as they will not get loaded or get loaded but not used. These modules occupy unnecessary storage space in the filesystem, and there are security concerns with too many unused modules. With kernel K5.15, DRIVE OS enables and copies only the essential kernel modules to the K5.15 root filesystem, which has known use cases. The kernel modules packaged in the filesystem currently for K5.15 is verified to be sufficient to cover the known use cases in DRIVE OS LINUX. The specific use case has issues if the customer has specific use cases on K5.15, which depend on kernel modules unavailable in the K5.15 filesystem that comes with SDK/PDK.

How does it impact the customer?

If the software used in your use case depends on the .ko file, then the software does not run.

If there is a workaround, what is it?

The below steps are not a workaround but a step to cover any specific customer use cases unknown to DRIVE OS LINUX. To add the missing *.ko files, copy them manually to the filesystem based on the steps below. Also, inform your customer support engineer of the use case for future kernel upgrades.

Use the steps below to copy all *.ko files in the SDK to the K5.15 RFS (including those not in the K5.15 copytarget YAML).

Case-1: If the additional modules are built and available in the SDK but not copied to the RFS:

- `$ export PROD_SUFFIX=<str>` # where <str> is empty string if using standard kernel or _prod if using production kernel
- Add the modules you want to copy to kernel modules YAML: `$NV_WORKSPACE/drive-linux/filesystem/copytarget/manifest/copytarget-kernel-modules.yaml`.
    - Quick start copytarget example is in the section System Software Components and Interfaces => DRIVE OS Linux Filesystems Customization Quick Start Page => Adding a Single Debian Package and a Single File to the Linux File System.
    - Copytarget API is documented in the section System Software Components and Interfaces => Copytarget => CopyTarget Manifest.
- Use the step from Compiling the Kernel (Kernel 5.15), step 11c (starts with "Copy the built modules to the root file system path with the following command"), to copy the modules to the RFS.

Case-2: If the modules are absent in `drive-linux/kernel/preempt_rt${PROD_SUFFIX}/modules/`, then the kernel defconfig must be changed to build the component as .ko and SDK kernel modules updated using the steps in the page "Kernel compilation in K5.15". After this step, the above copy steps must be used to copy the newly built .ko files.

Finally, please inform your customer support engineer of the use case so that the modules can be included in future DRIVE OS releases.

When can we expect the fix?

Additional NVIDIA-built modules can be included in the next DRIVE OS release (6.0.8.0) based on feedback from DRIVE OS customers.

Is it for SDK/PDK?

		Both
4079771	NvDisplay	**What is the issue?** HDMI is not enabled by default in AV+L build for any of devkit reference boards. **How does it impact the customer?** Platforms with HDMI connector output do not work by default. **If there is a workaround, what is it?** Follow the steps in the Enabling HDMI chapter under NvDisplay to enable HDMI on your board. **When can we expect the fix?** 6.0.8 **Is it for SDK/PDK?** Both
3885243	FSI	**What is the issue?** On production boards with no root key fused, the FSI keyblob from PSC is invalid and FSI SW is not able to parse it. FSI SW reports "ErrorCode-0x9 ReporterId-0x800d" to HSM. **How does it impact the customer?** Since provisioned keys are not anyway usable on non-fused boards, this is harmless and can be ignored. **If there is a workaround, what is it?** • In FSI closed box, this has been added to the "disable startup error" list. • In FSI open box, this error can be ignored through FSI code Eps_Cfg.h. **When can we expect the fix?** 6.0.8 **Is it for SDK/PDK?** Both
3953053	Kernel	**What is the issue?** `/sys/class/gpio` node has been deprecated in K5.15. **How does it impact the customer?** You can no longer use the GPIO sysfs (/sys/class/gpio). **If there is a workaround, what is it?** Use the "gpiod" tool (supported e.g., "gpioset" command) **When can we expect the fix?** The "gpiod" tool is already part of the kernel. **Is it for SDK/PDK?** It applies for K5.15 based packages (PDK/SDK).
4070042	Kernel	**What is the issue?** sestatus tool is not available in the Linux RFSes for Linux K5.15 while it is still available in RFSes for Linux K5.10. **How does it impact the customer?** You are not able to use sestatus in K5.15 DRIVE OS package. **If there is a workaround, what is it?** The same information can be extracted from other source such as /sys/fs/selinux/status. You can also `apt install policycoreutils` to get the

		command installed/supported on the target system.
		When can we expect the fix?
		6.0.8
		Is it for SDK/PDK?
		Both
4067922	FSI	**What is the issue?**
		FSISW Interrupt consistency check is not supported for 6.0.7.0.
		How does it impact the customer?
		In open box solution, missing timer interrupts in FSSIW GPT MCAL cannot be detected for GPT channels.
		For closed box solution, there is no impact as GPT channels are not configured and not used.
		If there is a workaround, what is it?
		N/A
		When can we expect the fix?
		6.0.8
		Is it for SDK/PDK?
		Both
3896536	System Software	**What is the issue?**
		tegra_bootloader_debug driver is broken with K5.15 because it is made a complete loadable module.
		How does it impact the customer?
		Any profiling use cases (such as boot time profiling) do not work by default with DRIVE Linux + K5.15.
		Note that there is no such issue on DRIVE Linux + K5.10.
		If there is a workaround, what is it?
		The workaround is to compile part of the driver as built-in instead of a loadable module:
		• Stop compiling tegra_bootloader_debug_init.c from kernel/nvidia-oot/drivers/platform/tegra/Makefile.
		• Continue compiling tegra_bootloader_debug.c from kernel/nvidia-oot/drivers/platform/tegra/Makefile as a module. No change expected for code in tegra_bootloader_debug.c.
		• Compile tegra_bootloader_debug_init.c as builtin driver from K5.15 source code. E.g. from kernel/3rdparty/canonical/linux-jammy/kernel-source/drivers/platform/tegra/Makefile
		• obj-y += tegra_bootloader_debug_init.o
		When can we expect the fix?
		6.0.8
		Is it for SDK/PDK?
		Both
4072102	AURIX	**What is the issue?**
		Multiple clients are communicating with Aurix over socket port 5001. One client is the MCC daemon using local IP address 0.0.0.0; there can be other clients linking with libmcu_common_if.so to communicate with Aurix via socket APIs. The clients linking with libmcu_common_if.so and communicating directly over socket port

		5001 may see a conflict and timeout error if they are launched using root user.
		How does it impact the customer?
		The clients linking with libmcu_common_if.so may see conflict with MCC daemon for the port 5001 if they are launched as root user.
		If there is a workaround, what is it?
		The clients linking with libmcu_common_if.so should be launched as non-root user.
		When can we expect the fix?
		N/A
		Is it for SDK/PDK?
		Both
3917664	Camera Core	**What is the issue?**
		Due to an issue with CSI calibration during capture start, a camera application using SIPL may see intermittent failures to start captures and see no frames being received by the application.
		How does it impact the customer?
		The impact to customers is limited to repeatedly launching and exiting a camera application. The intermittency rate is ~3-5%. The application can be launched again even after a failure to successfully start a new capture session most times.
		If there is a workaround, what is it?
		Yes, the workaround is to increase the deserializer MIPI speed for CPHY mode from 2000 MHz to 2500 MHz. The workaround has been merged on 6.0.7.0 branch for both Linux and QNX. On QNX safety, where this information is directly populated in the PlatformCfg struct, an example change has been made for the nvsipl_sample application to increase the MIPI speed for AR0820, IMX728 and IMX623 configurations used by that application.
		When can we expect the fix?
		6.0.8
		Is it for SDK/PDK?
		Linux SDK.
4068649	DRIVE Update	**What is the issue?**
		In AV+L, if SC7 happens when there is a DRIVE Update deployment ongoing, the deployment may fail after system resume; rate: 1/5.
		How does it impact the customer?
		Deployment via DRIVE Update may failed if SC7 happen, rate: 1/5.
		If there is a workaround, what is it?
		>Avoid SC7 when there is an ongoing deployment.
		When can we expect the fix?
		6.0.8.0.
3933195	DRIVE Update	**What is the issue?**
		Error logs such as "Error 0x2100004 on waitForReply from <path> to <path>" are printed in update VM when the system boots up.
		How does it impact the customer?
		No impact.
		If there is a workaround, what is it?
		N/A
		When can we expect the fix?

		6.0.8.0. **Is it for SDK/PDK?** All
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?** 6.0.8 **Is this Standard?** Issue is seen on Linux, PCT Configuration : AV+L **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
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
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
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?** 6.0.8 **Is it for SDK/PDK?** Linux SDK and PDK.
200775377	System Software	**What is the issue?** PTP client connected to DRIVE Orin AGX Developer Kit 88Q6113 (Spruce) ethernet switch 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.
200618961	System Software	**What is the issue?** Low fps observed while replaying sf3324/820 lraw/raw camera recordings with sample_camera_replay **How does it impact the customer?** Cannot replay sf3324/820 lraw/raw camera recordings smoothly via the Camera Replay Sample. **If there is a workaround, what is it?** N/A **When can we expect the fix?** N/A **Is it for SDK/PDK?** SDK
3925474		**What is the issue?** Header dump tool failed for lidar and radar with error: Could not cast to virtual sensor. [TC ID: 41643, 41645] **How does it impact the customer?** Cannot dump lidar/radar header by using header-dump

		If there is a workaround, what is it? N/A **When can we expect the fix?** Next release **Is it for SDK/PDK?** SDK
3929493		**What is the issue?** On x86, video not rendered properly after export from lraw/raw for AR0820, IMX728 Camera. Screen appeared in black color only. **How does it impact the customer?** Cannot use tool video_exporter to export mp4 files from AR0820/IMX728 raw/lraw recordings. **If there is a workaround, what is it?** N/A **When can we expect the fix?** N/A **Is it for SDK/PDK?** SDK
4064704		**What is the issue?** On x86, video replay of AR0820 camera sample_camera_replay/sample_camera is failed with error: DW_FAILURE: CameraMaster: camera not present in the NvSIPL database in use. **How does it impact the customer?** Cannot replay AR0820 raw recordings **If there is a workaround, what is it?** N/A **When can we expect the fix?** Next release **Is it for SDK/PDK?** SDK
4056215		**What is the issue?** On x86, video replay of hyp8 IMX623 camera with sample_camera_replay/sample_camera is getting hung and no renderer screen appeared. Pop-up window display asking for wait/force stop. **How does it impact the customer?** Cannot replay IMX623 raw recordings **If there is a workaround, what is it?** N/A **When can we expect the fix?** Next release **Is it for SDK/PDK?** SDK
4064784		**What is the issue?** sample_feature_descriptor fails with raw video input, Driveworks exception

		thrown: Bad access of safety result (underflow error) **How does it impact the customer?** Cannot run sample_feature_descriptor with raw video **If there is a workaround, what is it?** N/A **When can we expect the fix?** Next release **Is it for SDK/PDK?** SDK
	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		**What is the issue?** Sample_stereo_disparity dumps "Error calling GL deleter" on console **How does it impact the customer?** The same error log may occur during DriveWorks release. But it won't impact functionality. **If there is a workaround, what is it?** N/A **When can we expect the fix?** N/A **Is it for SDK/PDK?** SDK
		Tensor Streaming is not operational in this release.
200782352	SAL	LRAW Preview Extraction Tool fails.
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?
		6.0.8
		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.
6.0.7	Specifies the NVIDIA release branch number.
33194436	Specifies the build ID for the Linux operating system.
33194437	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.
5.10, 5.15	Specifies the supported kernel version(s).
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.	1.3

Safety systems are expected to use Vulkan SC.	
Vulkan SC	1.0
OpenWF Display	1.0
DriveWorks	5.12
DLA	3.13.0[1]
CUDA	11.4.22
cuDNN	8.9.0
TensorRT	8.6.10
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 11.4.22. 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. 366	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
cuobjdump	11.4. 366	Linux (aarch64), Linux (x86_64)
CUPTI	11.4. 366	Linux (aarch64), Linux (x86_64), qnx-

---

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

		standard_aarch64
CUDA cuxxfilt (demangler)	11.4. 366	Linux (aarch64), Linux (x86_64)
CUDA Demo Suite	11.4. 366	Linux (x86_64)
CUDA GDB	11.4. 366	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA NVCC	11.4. 366	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA nvdisasm	11.4. 366	Linux (aarch64), Linux (x86_64)
CUDA NVML Headers	11.4. 366	Linux (aarch64), Linux (x86_64)
CUDA nvprof	11.4. 366	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA nvprune	11.4. 366	Linux (aarch64), Linux (x86_64)
CUDA NVRTC	11.4. 366	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA NVTX	11.4. 366	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA NVVP	11.4. 366	Linux (x86_64)
CUDA Samples	11.4. 368	l4t_aarch64, Linux (aarch64), Linux (x86_64)
CUDA Compute Sanitizer API	11.4. 366	Linux (aarch64), Linux (x86_64)
CUDA Thrust	11.4. 366	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA cuBLAS	11.6.6.150	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA cuDLA	11.4. 366	Linux (aarch64), qnx-standard_aarch64
CUDA cuFFT	10.6.0.270	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA cuRAND	10.2.5.365	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA cuSOLVER	11.2.0.365	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA cuSPARSE	11.6.0.365	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
CUDA NPP	11.4.0.355	Linux (aarch64), Linux (x86_64), qnx-standard_aarch64
Nsight Compute	2021.2.9.1	Linux (x86_64), qnx-standard_aarch64
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