Predisclosure Security Bulletin: GPU Display Driver - February 2024

Document History

TB-07069-044_OEM_v1.0

Version	Date	Authors	Description of Change
1.0	January 9, 2024	PSIRT	Initial release
2.0	January 30, 2024	PSIRT	Added R550 driver versions and changed the title of the document to add February, replacing January
3.0	February 26, 2024	PSIRT	Changed embargo date to February 28, 2024

Table of Contents

Partner Security Bulletin: GPU Display Driver – February, 2024

This document is a notification provided under NDA and is not to be shared or disclosed to third parties without prior written approval from NVIDIA.

It is provided to recipients that use NVIDIA products and describes a vulnerability assessment for NVIDIA GPU hardware or software. It highlights specific instances that partners may wish to examine in the context of their operating environments.

The NVIDIA risk assessment is based on an average of risk across a diverse set of installed systems and may not represent the true risk to your local installation. Evaluating all possible system configurations is beyond the scope of this bulletin. NVIDIA recommends consulting a security or IT professional to evaluate the risk to your specific configuration.

Statements made in this document are valid at the time of publication and may not extend reliably into the future as the nature of the security issue evolves.

Embargo Notice

NVIDIA expects these issues, and the associated updates for these issues, to be disclosed in a public security bulletin posted to the NVIDIA Product Security page on **February 28, 2024** (9:00 AM PST) ("Disclosure Date"). Please coordinate any public discussion or disclosure, and release of these issues or the updates of these issues to align with our public security bulletin.

These issues must not be publicly discussed, disclosed, or otherwise released, nor the associated updates released, to any third party, including, but not limited to partners, before the Disclosure Date without prior written approval from NVIDIA. Additionally, prior to the Disclosure Date, partners must not reveal the affected components, even during testing of the updates, except to internal employees, or third-party testers under NDA, that have a need to know.

The NVIDIA public Disclosure Date is subject to change with little or no notice.

Details

This section provides a summary of potential vulnerabilities that this security update addresses and their impact. Descriptions use CWE™, and base scores and vectors use CVSS v3.1 standards.

NVIDIA GPU Display Driver

CVE ID	Description	Vector	Base Score	Severity	CWE	Impacts
CVE-2024-0071	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user mode layer, where an unprivileged regular user can cause an out-of-bounds write. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	7.8	High	CWE 125	Code execution, denial of service, escalation of privileges, information disclosure, data tampering

CVE ID	Description	Vector	Base Score	Severity	CWE	Impacts
CVE-2024-0073	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer when performing an operation at a privilege level that is higher than the minimum level required. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8	High	CWE-250	Code execution, denial of service, escalation of privileges, information disclosure, data tampering
CVE-2024-0074	NVIDIA GPU Display Driver for Linux contains a vulnerability where an attacker may access a memory location after the end of the buffer. A successful exploit of this vulnerability may lead to denial of service and data tampering.	AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H	7.1	High	CWE-788	Denial of service, data tampering
CVE-2024-0078	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a user in a guest can cause a NULL-pointer dereference in the host, which may lead to denial of service.	AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H	6.5	Medium	CWE-476	Denial of service

CVE ID	Description	Vector	Base Score	Severity	CWE	Impacts
CVE-2024-0075	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability where a user may cause a NULL-pointer dereference by accessing passed parameters the validity of which has not been checked. A successful exploit of this vulnerability may lead to denial of service and limited information disclosure.	AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.1	Medium	CWE-476	Denial of service, limited information disclosure
CVE-2022-42265	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an unprivileged regular user can cause integer overflow, which may lead to denial of service, information disclosure, and data tampering.	AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L	5.3	Medium	CWE-190	Denial of service, information disclosure, and data tampering

NVIDIA vGPU Software

CVE ID	Description	Vector	Base Score	Severity	CWE	Impacts
CVE-2024-0077	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, where it allows a guest OS to allocate resources for which the guest OS is not authorized. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8	High	CWE-285	Code execution, denial of service, escalation of privileges, information disclosure, data tampering
CVE-2024-0079	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a user in a guest can cause a NULL-pointer dereference in the host. A successful exploit of this vulnerability may lead to denial of service.	AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H	6.5	Medium	CWE-476	Denial of service

Security Updates for NVIDIA GPU Display Driver

CVE IDs Addressed in Each Windows Driver Branch

The following table lists the CVE IDs addressed by the update in each Windows driver branch.

Windows Driver Branch	CVE IDs Addressed

R550, R545, R535	CVE-2024-0071, CVE-2024-0073, CVE-2024-0078, CVE-2024-0075,
R470	CVE-2024-0071, CVE-2024-0073, CVE-2024-0078, CVE-2022-42265

The following table lists NVIDIA software products and driver versions affected, and the updated version that includes this security update.

Security Updates for NVIDIA GPU Display Driver for Windows

Software Product	Operating System	Driver Branch	Affected Driver Versions	Updated Driver Version	Partner Availability
GeForce	Windows	R550	All driver versions prior to 551.34	551.34	Available in the week of 1/29
		R545	All driver versions prior to 546.59	546.59	Available in the week of 1/8
		R535	All driver versions prior to 538.18	538.18	Available in the week of 1/8
	Windows 10 and 11	R470	All driver versions prior to 474.80	474.80	Available in the week of 1/8
	Windows 7 and 8.x	R470	All driver versions prior to 474.80 for support of GeForce Kepler desktop	474.80	Available in the week of 1/8
NVIDIA RTX, Quadro, NVS	Windows	R550	All driver versions prior to 551.34	551.34	Available in the week of 1/29
		R535	All driver versions prior to 538.18	538.18	Available in the week of 1/8
		R470	All driver versions prior to 474.80	474.80	Available in the week of 1/8
Tesla	Windows	R550	All driver versions prior to 551.34	551.34	Available in the week of 1/29
		R535	All driver versions prior to 538.18	538.18	Available in the week of 1/8
		R470	All driver versions prior to 474.80	474.80	Available in the week of 1/8

CVE IDs Addressed in Each Linux Driver Branch

The following table lists the CVE IDs addressed by the update in each Linux driver branch.

Linux Driver Branch	CVE IDs Addressed
R550, R545, R535	CVE-2024-0074, CVE-2024-0075
R470	CVE-2024-0074, CVE-2022-42265

Security Updates for NVIDIA GPU Display Driver for Linux

The following table lists NVIDIA software products and driver versions affected, and the updated version that includes this security update.

Software Product	Operating System	Driver Branch	Affected Driver Versions	Updated Driver Version	Partner Availability
GeForce	Linux	R550	All driver versions prior to 550.49	550.49	Available in the week of 1/29
		R535	All driver versions prior to 535.158	535.158	Available in the week of 1/8
		R470	All driver versions prior to 470.237	470.237	Available in the week of 1/8
NVIDIA RTX, Quadro, NVS	Linux	R550	All driver versions prior to 550.49	550.49	Available in the week of 1/29
		R535	All driver versions prior to 535.158	535.158	Available in the week of 1/8
		R470	All driver versions prior to 470.237	470.237	Available in the week of 1/8
Tesla	Linux	R550	All driver versions prior to 550.49	550.49	Available in the week of 1/29
		R535	All driver versions prior to 535.158	535.158	Available in the week of 1/8
		R470	All driver versions prior to 470.237	470.237	Available in the week of 1/8

Notes:

- You may release the non-partner-preview GPU display drivers listed in this partner security bulletin after the embargo has been lifted.
- Versions listed above may be different than the versions listed in the public security bulletin.

Security Updates for NVIDIA vGPU Software

CVE IDs Addressed in Each Windows vGPU Driver Branch

The following table lists the CVE IDs addressed by the update in each Windows vGPU driver branch.

Windows Driver Branch	CVE IDs Addressed
R550, R535	CVE-2024-0071, CVE-2024-0073, CVE-2024-0074, CVE-2024-0075, CVE-2024-0078
R470	CVE-2024-0071, CVE-2024-0073, CVE-2024-0074, CVE-2024-0078, CVE-2022-42265

CVE IDs Addressed in Each Linux vGPU Driver Branch

The following table lists the CVE IDs addressed by the update in each Linux vGPU driver branch.

Linux Driver Branch	CVE IDs Addressed
R550, R535	CVE-2024-0074, CVE-2024-0075, CVE-2024-0078
R470	CVE-2024-0074, CVE-2024-0078, CVE-2022-42265

CVE IDs Addressed in Each vGPU Manager Driver Branch

The following table lists the CVE IDs addressed by the update in each vGPU Manager driver branch.

vGPU Manager Driver Branch	CVE IDs Addressed
R550, R535	CVE-2024-0073, CVE-2024-0074, CVE-2024-0075, CVE-2024-0077, CVE-2024-0078, CVE-2024-0079
R470	CVE-2024-0073, CVE-2024-0074, CVE-2024-0077, CVE-2024-0078, CVE-2022-4226

Affected and Updated Versions

The following table lists the NVIDIA software products affected, versions affected, and the updated version that includes this security update.

CVE-IDs Addressed	Software Product	Operating System	Affected Versions		Updated Driver Version	Partner Availability (for testing only)
			vGPU Software	Driver		
CVE-2024-0071 CVE-2024-0073 CVE-2024-0074 CVE-2024-0075 CVE-2024-0078 CVE-2022-42265	Guest driver	Windows	All versions prior to and including 16.2	537.70	538.18	Contact NVIDIA PM team
			All versions prior to and including 13.9	474.64	474.80	Contact NVIDIA PM team
CVE-2024-0074 CVE-2024-0075 CVE-2024-0078 CVE-2022-42265	Guest driver	Linux	All versions prior to and including 16.2	535.129.03	535.158	Contact NVIDIA PM team
			All versions prior to and including 13.9	470.223.02	470.237	Contact NVIDIA PM team
CVE-2024-0074 CVE-2024-0075 CVE-2024-0077 CVE-2024-0078 CVE-2024-0079 CVE-2022-42265	Virtual GPU Manager	Citrix Hypervisor, VMware vSphere, Red Hat Enterprise Linux KVM, Ubuntu	All versions prior to and including 16.2	535.129.03	535.158	Contact NVIDIA PM team
			All versions prior to and including 13.9	470.223.02	470.237	Contact NVIDIA PM team
CVE-2024-0073 CVE-2024-0074 CVE-2024-0075 CVE-2024-0077 CVE-2024-0078 CVE-2024-0079 CVE-2022-42265	Virtual GPU Manager	Azure Stack HCI	All versions prior to and including 16.2	537.70	538.18	Contact NVIDIA PM team

Notes:

- vGPU drivers at partner availability dates will not be certified drivers and are provided for partner testing purposes only. These drivers should not be shared publicly even after the embargo is lifted.
- Certified vGPU drivers will be available at a later date in the Enterprise Portal upon public availability.
- Versions listed above may be different from the versions listed in the public sSecurity bulletin.
- The table above may not be a comprehensive list of all affected supported versions or branch releases, and may be updated as more information becomes available.
- Earlier software GPU branch releases that support these products may also be affected. If you are using an earlier branch release for which an update version is not listed above, we recommend upgrading to the latest branch release.

Mitigations

None. See the Security Updates section for the version to install.

For More Information

If you have any questions regarding this bulletin, please contact your NVIDIA Program Manager.

Visit the NVIDIA Product Security page to learn more about the vulnerability management process followed by the NVIDIA Product Security Incident Response Team (PSIRT).

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.

Trademarks

NVIDIA, 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

NVIDIA Corporation | 2788 San Tomas Expressway, Santa Clara, CA 95051
http://www.nvidia.com