Security Bulletin

Vulnerability in NVIDIA GPU Display Driver

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-1742**
Created	:	**06 February 2025**
Version	:	**0.3**
Status	:	**Neutralization**
TLP Classification	:	**CLEAR**
Document date	:	**18 February 2025**
Keywords	:	**CVE-2024-0126 CVE-2024-0131 CVE-2024-0147 CVE-2024-0149 CVE-2024-0150 CVE-2024-53869**

TLP:CLEAR

FOR PUBLIC USE

FOR PUBLIC USE

TLP:CLEAR

Vulnerability in NVIDIA GPU Display Driver - CVE-2024-0126 CVE-2024-0131 CVE-2024-0147 CVE-2024-0149 CVE-2024-0150 CVE-2024-53869   **Eviden PSIRT**

List of changes

Version	Date	Description
0.1	2024/12/05	Initial Eviden version
0.2	2024/12/11	Added affected MPI version in table
0.3	2025/02/18	CVE-2024-0131 CVE-2024-0147 CVE-2024-0149 CVE-2024-0150 CVE-2024-53869 added to bulletin. TLP changed for CLEAR

Executive summary

NVIDIA reported information about NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability which could allow a privileged attacker to escalate permissions. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering. NVIDIA published table with lists the NVIDIA software products affected, Linux driver versions affected, and the updated version available from nvidia.com that includes this security update.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2024-0126	8.2	CWE-20 Improper Input Validation
CVE-2024-0131	4.4	
CVE-2024-0147	5.5	
CVE-2024-0149	3.3	
CVE-2024-0150	7.1	
CVE-2024-53869	5.5	

Eviden is liaising closely with its suppliers and investigating the exact nature of these vulnerabilities to provide validated remediation.

Affected products

Products	Fixed version	Status	Comments
Tesla p100	550.127.05 535.216.01	Fixed	Affected by CVE-2024-0126
Tesla p100	550.137 535.226	Fixed	Affected by CVE-2024-0131 CVE-2024-0147 CVE-2024-0149 CVE-2024-0150 CVE-2024-53869
RTX, Quadro	550.137 535.226	Fixed	Affected by CVE-2024-0131 CVE-2024-0147 CVE-2024-0149 CVE-2024-0150 CVE-2024-53869

FOR PUBLIC USE

TLP:CLEAR

Vulnerability in NVIDIA GPU Display Driver - CVE-2024-0126 CVE-2024-0131 CVE-2024-0147 CVE-2024-0149 CVE-2024-0150 CVE-2024-53869

Eviden PSIRT

Although Eviden tries to provide accurate and complete information, Eviden shall not be liable if the above table is incomplete or erroneous. During its vulnerability analysis process, the information in this document is subject to change without notice to reflect new results of this analysis.

The tables below provide the Technical State to apply to implement the fixes on Eviden products.

Note: The first row provides the currently recommended combination of firmware. The detail per vulnerability is given below.

TS (technical state) with no number indicates that a new technical state fixing the vulnerabilities is scheduled.

TBD (to be defined) indicates that a new technical state fixing the vulnerabilities is under study.

Unpatched means that the vulnerability is presumably present, but there is no plan to provide a fix. This can be investigated on demand.

List of Enterprise and Edge servers

Products	Fixed version	Comment
BullSequanaSA	Unpatched	fix is related to driver update

List of HPC products

Products	Fixed version	Comment
BullSequanaX400-A5	Unpatched	fix is related to driver update
BullSequanaX400-E5	Unpatched	fix is related to driver update

Recommendations

Eviden recommends applying its Technical States upgrade on its servers as soon as they are made available.

Available Vendor Patches

No validated patch is available at the time. Eviden is working with its suppliers to distribute updates as soon as possible.

The following table lists the NVIDIA software products affected, Linux driver versions affected, and the updated version available from nvidia.com that includes this security update. Download the updates from the NVIDIA Driver Downloads page.

FOR PUBLIC USE

TLP:CLEAR

Vulnerability in NVIDIA GPU Display Driver - CVE-2024-0126 CVE-2024-0131 CVE-2024-0147 CVE-2024-0149 CVE-2024-0150 CVE-2024-53869

Eviden PSIRT

Software Product	Operating System	Driver Branch	Affected Driver Versions	Updated Driver Version
GeForce	Linux	R565	All driver versions prior to 565.57.01	565.57.01
		R550	All driver versions prior to 550.127.05	550.127.05
		R535	All driver versions prior to 535.216.01	535.216.01
NVIDIA RTX, Quadro, NVS	Linux	R565	All driver versions prior to 565.57.01	565.57.01
		R550	All driver versions prior to 550.127.05	550.127.05
		R535	All driver versions prior to 535.216.01	535.216.01
Tesla	Linux	R550	All driver versions prior to 550.127.05	550.127.05
		R535	All driver versions prior to 535.216.01	535.216.01

Affected	NVIDIA Driver	Delivery HPC
OpenMPI4 OpenMPI5	560.35.03	1261.0.8
OpenMPI4 OpenMPI5	555.42.06	1251.0.1
OpenMPI4	545.23.08	1232.0.1
OpenMPI4	535.10.4.05	12.1.7

Technical States links for Eviden servers are reminded in the table below.

Product	Technical State link
Bull Sequana S	https://support.bull.com/ols/product/platforms/bullion/bullsequana-s/dl/pkgf/technical-state-dvd-packages
Bull Sequana SA	https://support.bull.com/ols/product/platforms/bullion/bullsequana-sa-servers/dl/pkgf/pkg
Bull Sequana SH	https://support.bull.com/ols/product/platforms/bullion/bullsequana-sh/dl/pkgf/pkg
Bull Sequana E	https://support.bull.com/ols/product/platforms/bullion/bullsequana-edge-servers/dl/pkgf/pkgf
Bull Sequana X1000	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x1000/dl/pkgf/pkg
Bull Sequana XH2000	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/xh2000/dl/pkgf/pkg
Bull Sequana XH3000	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/xh3000/dl/pkgf/pkg
Bull Sequana X400-E5	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkgx400e5
Bull Sequana X400-E7	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkgx400e7
Bull Sequana X400-A5	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkgx400a5
Bull Sequana X400-A6	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkgx400a6
Bull Sequana X550	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x550

FOR PUBLIC USE

TLP:CLEAR

Vulnerability in NVIDIA GPU Display Driver - CVE-2024-0126 CVE-2024-0131 CVE-2024-0147 CVE-2024-0149 CVE-2024-0150 CVE-2024-53869

Eviden PSIRT

Bull Sequana X800 / QLM	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x800/dl/pkgf/pkg

Available Workarounds

No workaround is available.

Available Mitigations

No mitigation identified.

Available Exploits/PoC

Eviden is not aware of any exploitation of the reported vulnerabilities.

References

1. https://nvidia.custhelp.com/app/answers/detail/a_id/5586

FOR PUBLIC USE

TLP:CLEAR

**Vulnerability in NVIDIA GPU Display Driver - CVE-2024-0126 CVE-2024-0131
CVE-2024-0147 CVE-2024-0149 CVE-2024-0150 CVE-2024-53869**

Eviden
PSIRT

Glossary of terms

Term	Description
Mitigation	Refers to a setting, common configuration, or general best-practice, existing in a default state that could reduce the severity of exploitation of a vulnerability
Neutralization	The neutralization phase is the decision-making process during which the risk posed by an incident is evaluated.
PoC	Proof of Concept
Remediation	The remediation phase ends with the delivering of a qualified solution/update fixing the vulnerability without regression.
TI	Threat Intelligence
TLP	Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0. https://www.first.org/tlp/
Workaround	Refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update

About this document

Eviden continuously monitors the security of its products. This Security Bulletin is shared under the constraints of the FIRST Traffic Light Protocol version 2.0 (TLP) to bring the attention of owners of the potentially affected Eviden products. Eviden recommends that all product owners determine whether the described situation is applicable to their individual case and take appropriate action.

Although Eviden tries to provide accurate and complete information, Eviden shall not be liable for technical or editorial errors contained in this Bulletin. The information is provided "as is" without warranty of any kind. To the extent permitted by the Law, neither Eviden nor its affiliates, subcontractors or suppliers will be liable for incidental damages, downtime cost, lost profits, damages relating to the procurement of substitute products or services, or damages for loss of data, or software restoration. Product and company names mentioned herein may be trademarks of their respective owners.

The information in this document is subject to change without notice. The version of this document will be incremented according to the changes:

- Neutralization security bulletins are numbered 0.x
- Privately disclosed Remediation security bulletins are numbered 1.x
- Publicly disclosed Remediation security bulletins are numbered 2.x

Updated versions of this document can be found on:

- https://support.bull.com/ols/product/security/psirt

FOR PUBLIC USE

TLP:CLEAR

| Vulnerability in NVIDIA GPU Display Driver - CVE-2024-0126 CVE-2024-0131 CVE-2024-0147 CVE-2024-0149 CVE-2024-0150 CVE-2024-53869 | Eviden PSIRT |

About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

About Eviden[1]

Eviden is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 53,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

---

[1] Eviden business is operated through the following brands: AppCentrica, ATHEA, BullSequana, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, IDnomic, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Trustway, Visual BI, Worldgrid, X-Perion.
Eviden is a registered trademark. © Eviden SAS, 2025.