EVIDEN
an atos business

Security Bulletin

Vulnerability in AMD (GPU Kernel)

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-1018**
Created	:	**14 June 2024**
Version	:	**0.8**
Status	:	**Neutralization**
TLP Classification	:	**CLEAR**
Document date	:	**20 November 2024**
Keywords	:	**CVE-2023-4969 CVE-2023-51042 CVE-2024-21969**

TLP:CLEAR

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

FOR PUBLIC USE

List of changes

Version	Date	Description
0.1	2024/01/29	Initial neutralization version
0.2	2024/02/04	Added link to AMD bulletin
0.3	2024/04/05	No significant change.
0.4	2024/05/24	CVE-2023-51042 added to bulletin. Updated list of affected products.
0.5	2024/06/26	CVE-2024-21969 added to bulletin
0.6	2024/10/02	Added note about recommendation
0.7	2024/10/17	TLP changed for CLEAR
0.8	2024/11/20	Added fix version for MI300A

Executive summary

Researchers from Trail of Bits reported a potential vulnerability, titled "LeftoverLocals." According to their research, a compromised GPU kernel could potentially read local memory values from another kernel. The vulnerability affects, among others, AMD Instinct™ MI250 and AMD Instinct™ MI300A which are embedded in some BullSequana products - CVE-2023-4969

A use-after-free flaw was found in the Linux kernel's AMD GPU driver which may allow access to members of a synchronization structure after the structure is freed. This issue could allow a local user to crash the system or to access confidential system memory - CVE-2023-51042

Researchers from Technische Universitat Berlin have published a paper titled "Whispering Pixels." According to their research, improper register initialization routines could allow pixel data to be retained in GPU register storage before shader execution. This data could potentially be read using a specially crafted shader, potentially leading to cross-process information leakage. - CVE-2024-21969

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2023-4969	6.5	CWE-401 -Missing Release of Memory after Effective Lifetime
CVE-2023-51042	7.8	CWE-416 - Use After Free
CVE-2024-21969	6.5	TBD

CVE-2023-4969

Trail Of Bits has published an extensive explanation on its blog for the discovered vulnerability identified as CVE-2023-4969. It allows you to steal data from the local memory of the graphics card.

The reason for the problem is that the software running on GPU cards does not isolate the device's memory well enough and one kernel is able to read data written by another.

To successfully exploit the vulnerability, the attacker must be on the same machine and be able to run an application that uses the GPU for computation. Researchers here mention OpenCL, Vulkan or Metal, among others, as frameworks that will allow you to create a GPU kernel that will simply dump the uninitialized local memory of the card. Under normal conditions, reading uninitialized memory has no specific effect (so-called UB - undefined behavior), in the case considered by the researchers, this action leads to information leakage. It was also noted that frameworks used by web browsers (e.g. WebGPU) cannot be used to obtain another user's information because they implement dynamic memory checks in kernels.

CVE-2023-51042

This issue is only applicable to the amdgpu module, which is typically only loaded on systems that use AMD GPU hardware. Use the lsmod command to determine whether the amdgpu module is loaded.

CVE-2024-21969

Improper clearing of GPU registers could allow an attacker using a malicious shader to read left-over pixel data, potentially leading to loss of confidentiality.

Affected products

Products	Fixed version	Status	Comments
AMD Instinct™ MI250	TBD	Affected	No firmware patch. Recommended apply driver updated from AMD.
AMD Instinct™ MI300A	ROCm 6.2.4	Affected	No firmware patch. Recommended apply driver updated from AMD.

Although Eviden makes effort 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 current 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

Enterprise and Edge servers are not affected by these vulnerabilities.

List of HPC products

BullSequana X80x, X500-E5, X816, XH1000, and XH2000 series are not affected.

CVE	CVSS Score	Bull Sequana X410-A5 2U1N2S-4GPUs-ALD	Bull Sequana XH3406
Recommended		N/A	N/A
CVE-2023-4969	6.5	Unpatched	Unpatched
CVE-2023-51042	7.8	Unpatched	Unpatched
CVE-2024-21969	6.5	Unpatched	Unpatched

Recommendations

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

AMD plans to create a new mode that prevents processes from running in parallel on the GPU and clears local memory between processes on supported products. This mode would be designed to be set by an administrator and not enabled by default. Supporting documentation for the new mode, along with details of how to update AMD products, will be provided in a future update to this security notice.

AMD expects to start rolling out mitigation options beginning in March 2024 through upcoming driver updates.

No firmware patch. Recommended apply driver updated from AMD.

Available Vendor Patches

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

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

Product	Technical State link
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 X400-E5	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkg
Bull Sequana X400-A5	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400-a5/dl/pkgf/pkg
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 this vulnerability.

The vulnerability PoC has been published in the Github repository.

https://github.com/trailofbits/LeftoverLocalsRelease

References

1. https://nvd.nist.gov/vuln/detail/CVE-2023-4969
2. https://github.com/trailofbits/LeftoverLocalsRelease
3. https://kb.cert.org/vuls/id/446598
4. https://blog.trailofbits.com/
5. https://registry.khronos.org/OpenCL/specs/3.0-unified/html/OpenCL_API.html#_fundamental_memory_regions

6. https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html
7. https://www.amd.com/en/resources/product-security/bulletin/amd-sb-6010.html
8. https://nvd.nist.gov/vuln/detail/CVE-2023-51042
9. https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.4.12
10. https://github.com/torvalds/linux/commit/2e54154b9f27262efd0cb4f903cc7d5ad1fe9628
11. https://access.redhat.com/security/cve/CVE-2023-51042
12.

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 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 makes effort to provide accurate and complete information, Eviden shall not be liable for technical or editorial errors contained in this Bulletin. The information provides 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

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, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Visual BI, Worldgrid, X-Perion. Eviden is a registered trademark. © Eviden SAS, 2023.