EVIDEN
an atos business

Security Bulletin

Side channels attacks on CPUs

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-1133**
Created	:	**19 September 2022**
Version	:	**2.12**
Status	:	**Remediation**
TLP Classification	:	**CLEAR**
Document date	:	**8 May 2025**
Keywords	:	**CVE-2021-26341, CVE-2021-26401, CVE-2021-46744, CVE-2021-46778, CVE-2022-0001, CVE-2022-0002, CVE-2022-23816, CVE-2022-23823, CVE-2022-23825, CVE-2022-24436, CVE-2022-28693, CVE-2022-29900, CVE-2022-29901, CVE-2024-2193, CVE-2024-2201**

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
2.0	2022/10/05	First public version (https://atos.net/en/lp/securitydive/side-channel-attacks-on-cpu)
2.1	2024/03/17	Initial Eviden version. Adding CVE-2022-26373, CVE-2024-2193. Revision of product tables according to updated information and CPU ID.
2.2	2024/03/25	Adding amd-sb-7021 bulletin (Zenhammer)
2.3	2024/04/12	Adding amd-sb-7018 bulletin (CVE-2024-2201)
2.4	2024/04/26	Adding reference to Intel's recommendation for CVE-2024-2201
2.5	2024/05/03	Adding amd-sb-7015 bulletin (Exploiting the Conditional Branch Predictor) Adding note relative to SLAM attack.
2.6	2024/08/30	Adding note (CounterSEVeillance: Performance-Counter Based Control-Flow Recovery Attacks on AMD SEV-SNP) Adding amd-sb-7015 to bulletin
2.7	2024/10/31	Adding AMD-SN-7024 to bulletin, adding AMD-SN-7025 to bulletin
2.8	2024/11/13	Adding AMD-SN-7031
2.9	2025/02/03	Adding AMD-SN-3010
2.10	2025/02/11	Adding AMD-SN-7032
2.11	2025/04/02	Adding AMD-SN-7040 and AMD-SN-7026
2.12	2025/05/08	Adding AMD-SN-7042 and AMD-SN-7034

Executive summary

Regularly, new side-channel vulnerabilities are published affecting CPUs from Intel or AMD, some of which being used in Eviden products. This bulletin updates a previous document aiming at clarifying the status of Eviden products relatively to these vulnerabilities.

Due to the very nature of this class of vulnerabilities, standard patching measures do not apply. In some cases, mitigation can exist which may at some point degrade general performance. The purpose of this document is to summarize these vulnerabilities and provide references to some mitigation measures as published by CPU vendors.

Vulnerability Info

Principle

Side-channel attacks have no impact on integrity or availability. They may only have an interest when they give access to some important confidential information such as a cryptographic secret. Exploitation in other circumstances is unlikely. From a risk analysis perspective, a side-channel attack will therefore have an interest if and only if:

1. A CPU is used in a legitimate way to perform some cryptographic operation on behalf of a legitimate actor Alice.

2. The same CPU is used by a malevolent actor Eve at the same time.

Of course, the side-channel attack's interest resides in the fact that Eve will only use legitimate access to obtain information on Alice's secret. No elevation of privilege is performed. It is the influence of Alice's processus on Eve's processus which will leak sensitive information that Eve can leverage.

Risk analysis

Under the above prerequisites, a risk analysis is likely to overestimate the impact of a side-channel vulnerability if it places the attack scenario in the context of a cryptographic security module. A generic CPU is designed for performance. Hence, side-channel attack on generic CPU should not be considered as effective as they are on a Cryptographic security module. Using the CVSS v3.1 reference, we therefore consider the following in the context of a CPU used for generic purpose on an Eviden server.

- **Access Vector: Network**. There is no restriction in using this kind of vulnerability remotely. Example scenarios involve cloud-based infrastructure and virtual machines.

- **Attack Complexity: High**. Even though side-channel attacks can be made reproducible in laboratory, their implementation in true environment relies on some conditions which are out of reachof the attacker.

- **Privilege Required: Low**. By definition, a side-channel exploitation on a CPU requires the right to execute some computation on the CPU aside the target one. But no elevation of privilege is required.

- **User Interaction: None**. This may be debatable, because in some case, some sort of synchronization needs to be performed. But we consider here the worst-case scenario.

- **Scope: Unchanged**. This is also debatable because the accessed secret may be used to several usages. But we consider the scope unchanged because the secret must be processed by the vulnerable component (the CPU) for the side-channel attack to be successful.

- **Confidentiality Impact: Low**. Here again, this is debatable. But the existence of a side-channel vulnerability in a CPU doesn't mean in any way that any secret computed by the CPU can be accessed. The proof-of-concept of the vulnerability usually implements both Alice and Eve computations to evidence that Eve can access Alice's secret. But this highly depends on the

way Alice implements its computation, as can be seen by the mitigation guidelines provided by CPU vendors.

- **Integrity Impact: None**.
- **Availability Impact: None**.
- **Exploit Code Maturity**: Proof-of-Concept code. This is the usual case of research paper. In some case, side-channel weaknesses can also be inferred from design analysis, in which case no proof of exploit really exists.
- **Remediation Level**: Workaround. As seen below, the CPU vendors have published guidelines to mitigate the side-channel attacks which could be used on their CPUs.
- **Report Confidence: Confirmed**. As soon as CPU vendors have issued an advisory, we consider the vulnerability as confirmed.

As a result of this analysis, the Overall CVSS score of a side-channel CPU vulnerability is considered as Low (2.9).

CVSS Vector: AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:W/RC:C

Affected products

Vulnerabilities affecting AMD CPUs

CVE	AMD Bulletin	Type of vulnerability
CVE-2021-26341	amd-sb-1026	Speculative execution
CVE-2021-26401	amd-sb-1036	Speculative execution
CVE-2021-46744	amd-sb-1033	Ciphertext side-channel
CVE-2021-46778 (SQUIP channel)	amd-sb-1039	Contention-based side channel
CVE-2022-23823 (Hertzbleed)	amd-sb-1038	Timing attack using frequency scaling due to CPU throttling.
CVE-2022-29900 (RETbleed - aka CVE-2022-23816) CVE-2022-23825	amd-sb-1037	Branch type confusion
CVE-2024-2193	amd-sb-7016	Speculative Race Conditions (SRCs)
TBD	amd-sb-7021	Rowhammer attack on DDR4 and DDR5 memory on AMD Zen CPU based platform
CVE-2024-2201	amd-sb-7018	Not applicable according to AMD statement
TBD	amd-sb-7015	Exploiting the Conditional Branch Predictor
TBD	amd-sb-7024.html	Self-Modifying Code
TBD	amd-sb-7025.html	Principled Microarchitectural Isolation on Cloud CPUs
TBD	amd-sb-7031.html	“Speculative Return Stack Overflow”
TBD	amd-sb-3010.html	Cache coherency policy on AMD SEV
TBD	amd-sb-7032.html	Last-level cache attacks are practical in AMD Zen Processors
TBD	amd-sb-7040.html	Page prefetcher attack (PPA)
TBD	amd-sb-7026.html	Branch History Leak
TBD	amd-sb-7034.html	Domain Isolation
TBD	amd-sb-7042.html	IOLeak Exploiting CPU Frequency Scaling and I/O Latency

Vulnerabilities affecting Intel CPUs

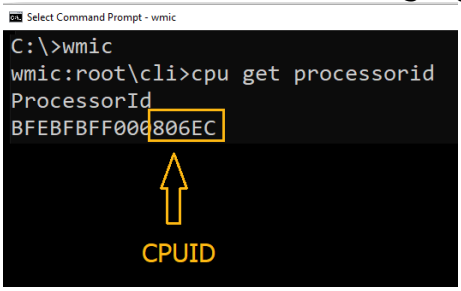
CVE	Intel Bulletin	Type of vulnerability
CVE-2022-0001 CVE-2022-0002 CVE-2024-2201	intel-sa-598	Branch prediction. See update of Intel’s recommendation relatively to BHI (CVE-2024-2201)

CVE	Intel Bulletin	Type of vulnerability
CVE-2022-24436 (Hertzbleed)	intel-sa-666	Timing attack using frequency scaling due to CPU throttling.
CVE-2022-26373 CVE-2022-28693 (Retbleed)	intel-sa-706 intel-sa-707	Branch type confusion For more details, see dedicated Eviden bulletin "Intel Processors RRSBA Advisory"
CVE-2022-29901	intel-sa-702	Branch type confusion

The products are affected according to the precise versions of processor embedded. The Intel processors report their precise version through the CPUID instruction.

Windows operating systems

Follow Intel's instruction to get your CPUID. The CPUID is part of the processor ID.



Linux operating systems

To obtain the CPUID of your Intel CPU, use the following command.

```
lscpu | awk '\
($1 == "Model:"){m1=$2/16; m2=$2%16}\
($1 == "Stepping:"){step=$2}\
($1 " " $2 == "CPU family:"){family=$3}\
END{printf("%.1x%.2x%.1x%.1x\n",m1,family,m2,step)} '
```

```
$ lscpu | awk '\
($1 == "Model:"){m1=$2/16; m2=$2%16}\
($1 == "Stepping:"){step=$2}\
($1 " " $2 == "CPU family:"){family=$3}\
END{printf("%.1x%.2x%.1x%.1x\n",m1,family,m2,step)} '
806ec
$
```

List of affected CPUID

The reference for affected CPUID is Intel's consolidated list of affected processors. The affected CPUID that you may find in BullSequana platforms are of the following type:

Component name	CPUID	Status	Vulnerabilities

Haswell	306F2, 306F4	Not affected	
Broadwell	406F1	Not affected	
Skylake	50653, 50654	Unpatched	CVE-2022-29901
Cascade Lake	50656, 50657	Unpatched	CVE-2022-0001, CVE-2022-0002, CVE-2022-26373, CVE-2022-28693
Broadwell DE	50663, 50664, 50665	Not affected	
Ice Lake Xeon-SP	606A6	Unpatched	CVE-2022-0001, CVE-2022-0002, CVE-2022-26373
Ice Lake D	606C1	Unpatched	CVE-2022-0001, CVE-2022-0002, CVE-2022-26373
Sapphire Rapids	806F7	Unpatched	CVE-2022-0001, CVE-2022-0002, CVE-2022-26373, CVE-2022-28693
Sapphire Rapids HBM	806F8	Unpatched	CVE-2022-0001, CVE-2022-0002, CVE-2022-26373, CVE-2022-28693
Emerald Rapids	C06F2	Unpatched	CVE-2022-28693, CVE-2022-26373

Note on some of the side-channel attacks

- Regarding the SLAM attack described by the VUSec research group (https://www.vusec.net/projects/slam/) no mitigation at hardware level is envisioned:
  - AMD pointed to current Spectre v2 mitigations to address and did not provide any guidance or updates that would lower the risk.
  - Intel announced plans for providing software guidance before releasing future processors that support LAM, such as deploying the feature with the Linear Address Space Separation (LASS) security extention for preventing speculative address accesses across user/kernel mode.

Note of paper titled “CounterSEVeillance: Performance-Counter Based Control-Flow Recovery Attacks on AMD SEV-SNP.”

- Researchers from Graz University of Technology, Austria, have reported a way for a malicious hypervisor to monitor performance counters and potentially recover data from a guest Virtual Machine (VM). In their paper, the researchers propose that it is possible for a malicious hypervisor to potentially exploit performance counters (PMCs) to leak data from a guest VM. They demonstrate an exploit that interrupts a guest VM after each instruction and examine PMC differences to determine the outcomes of conditional branches, highlighting the potentially serious impact of these vulnerabilities.
- AMD recommends software developers employ existing best practices, including avoiding secret-dependent data accesses or control flows where

appropriate to help mitigate this potential vulnerability. AMD has defined support for performance counter virtualization in APM Vol 2, section 15.39. PMC virtualization, planned for availability on AMD products starting with Zen 5, is designed to protect performance counters from the type of monitoring described by the researchers.

- Links:
  https://www.amd.com/content/dam/amd/en/documents/processor-tech-docs/programmer-references/24593.pdf
  https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/solution-briefs/amd-secure-encrypted-virtualization-solution-brief.pdf
  https://www.amd.com/content/dam/amd/en/documents/resources/glossary-of-terms.pdf

List of Enterprise and Edge servers

BullSequana Edge Series

BullSequana	Status	Remaining vulnerabilities
E	Unpatched	See Vulnerabilities affecting Intel CPUs
EXR		
EXD		

BullSequana M Series

BullSequana	Status	Remaining vulnerabilities
M7200	Unpatched	See Vulnerabilities affecting Intel CPUs
M9600		

BullSequana S Series

BullSequana	Status	Remaining vulnerabilities
S200	Unpatched	See Vulnerabilities affecting Intel CPUs
S400		
S800		
S1600		
Bullion S	Not affected	See Vulnerabilities affecting Intel CPUs

BullSequana SA Series

BullSequana	Status	Remaining vulnerabilities
SA10	Unpatched	See Vulnerabilities affecting AMD CPUs.
SA10EL		
SA10-NVMe		
SA20		
SA20-NVMe		
SA20G		
SA20G-NVMe		
SA11a		
SA21a		
SA21Sa		
SA11i	Unpatched	See Vulnerabilities affecting Intel CPUs
SA21i		
SA21Si		

BullSequana SH Series

BullSequana	Status	Remaining vulnerabilities
SH20 2S2U	Unpatched	See Vulnerabilities affecting Intel CPUs
SH40 4S4U		
SH80 6-8S8U		
SH160 10-16S19U		

List of HPC products

Bullx Series

Product	Status	Remaining vulnerabilities
Bullx B520	Not affected	See Vulnerabilities affecting Intel CPUs
Bullx DLC B720		
Bullx DLC B725		
Bullx R421 E4		
Bullx R421 E4k		
Bullx R425 E4		
Bullx R424 E4		
Bullx R424 E4j		
Bullx R423 E4i		
Bullx R423 E4j		
Bullx R423 E4m		
Bullx S “Supernode”		

BullSequana X400-A5 Series

BullSequana	Status	Remaining vulnerabilities
X410-A5 2U1N1S 4GPU	Unpatched	See Vulnerabilities affecting AMD CPUs.
X410-A5 2U1N2S 4GPU ALD		
X410-A5 2U1N2S 4GPU SXM		
X410-A5 2U1N2S 8GPU		
X430-A5 2U1N1S		
X430-A5 2U1N2S		
X440-A5 2U4N1S		
X440-A5 2U4N2S		
X450-A5 2U1N2S		

SMS Series

BullSequana	Status	Remaining vulnerabilities
SMC xScale Master / Worker	Unpatched	See Vulnerabilities affecting AMD CPUs.
SMC Server		

BullSequana X400-A6 Series

BullSequana	Status	Remaining vulnerabilities
X410-A6 4U1N2S 8G PCIe	Unpatched	See Vulnerabilities affecting AMD CPUs.
X430-A6 2U1N1s		
X430-A6 2U1N2S		
X440-A6 2U4N2S		
X450-A6 2U1N2S 2G		

BullSequana X400-E5 Series

BullSequana	Status	Remaining vulnerabilities
X410-E5 1U-1N PCIe	Unpatched	See Vulnerabilities affecting Intel CPUs
X410-E5 1U-1N NVLink		
X430-E5 2U-1N		
X430-E5 1U-1N		
X440-E5 2U-4N 3.5-HDD		
X440-E5 2U-4N 3.5-HDD ER		
X440-E5 2U-4N 3.5-HDD HR		
X440-E5 2U-4N 2.5-HDD		
X440-E5 2U-4N 2.5-HDD ER		
X440-E5 2U-4N 2.5-HDD HR		
X440-K5 2U-4N		
X450-E5 4U-1N		

BullSequana X400-E7 Series

BullSequana	Status	Remaining vulnerabilities
X430-E7 2U1N1S	Unpatched	See Vulnerabilities affecting Intel CPUs
X430-E7 2U1N2S		
X440-E7 2U4N2S		
X450-E7 2U1N2S 2G		

BullSequana X500-E5 Series

BullSequana	Status	Remaining vulnerabilities
X541-E5-R412810	Unpatched	See Vulnerabilities affecting Intel CPUs
X541-E5-R434C10		
X550-8U-IC-8PSR		

BullSequana X800 Series

BullSequana	Status	Remaining vulnerabilities
X802	Unpatched	See Vulnerabilities affecting Intel CPUs
X804		
X808		
X816		

BullSequana X1000 Series

BullSequana	Status	Remaining vulnerabilities
X1110	Non affected	See Vulnerabilities affecting Intel CPUs
X1120	Unpatched	See Vulnerabilities affecting Intel CPUs
X1125		

BullSequana XH2000 Series

BullSequana	Status	Remaining vulnerabilities
XH2135	Unpatched	See Vulnerabilities affecting Intel CPUs
XH2140		
XH2410	Unpatched	See Vulnerabilities affecting AMD CPUs.
XH2415		

BullSequana XH3000 Series

BullSequana	Status	Remaining vulnerabilities
XH3140	Unpatched	See Vulnerabilities affecting Intel CPUs
XH3145		
XH3420	Unpatched	See Vulnerabilities affecting AMD CPUs.

List of Quantum products

BullSequana	Status	Remaining vulnerabilities
QLM 30	Unpatched	See Vulnerabilities affecting Intel CPUs
QLM 35		
QLM 38		
QLM 39		
QLM 40		
QLM E		

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.

Unpatched means that the vulnerability is presumably present, but there is no plan to provide a fix.

Recommendations

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

Available Vendor Patches

Due to the nature of a side-channel weakness, no patch is to be expected at hardware level.

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

Available Workarounds

In some cases, the source of information resides in some extended CPU feature which can be disabled at kernel level. Eviden do not recommend applying these sort of workaround as it may impact the overall performance of the system.

Available Mitigations

The References section list some resources from CPU vendors to implement mitigation at application level.

Available Exploits/PoC

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

References

1. https://www.amd.com/system/files/documents/technical-guidance-for-mitigating-branch-type-confusion_v7_20220712.pdf
2. https://www.amd.com/system/files/documents/software-techniques-for-managing-speculation.pdf
3. https://www.amd.com/system/files/documents/221404394-a_security_wp_final.pdf
4. https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/advisory-guidance/return-stack-buffer-underflow.html
5. https://atos.net/en/lp/securitydive/side-channel-attacks-on-cpu
6. https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/technical-documentation/branch-history-injection.html
7. https://www.amd.com/content/dam/amd/en/documents/epyc-technical-docs/tuning-guides/software-techniques-for-managing-speculation.pdf
8. https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7026.html

9. http://amd.com/en/resources/product-security/bulletin/amd-sb-7034.html
10. http://amd.com/en/resources/product-security/bulletin/amd-sb-7042.html
11.

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

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.