EVIDEN
an atos business

Security Bulletin

Gather Data Sampling vulnerability in Intel CPUs

Author(s)	:	Eviden PSIRT
Reference	:	PSIRT-535
Created	:	28 August 2023
Version	:	2.11
Status	:	Remediation
TLP Classification	:	CLEAR
Document date	:	1 July 2024
Keywords	:	CVE-2022-40982

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	2023-08-21	First draft version
0.2	2023-08-30	First neutralization version
~~0.2.1~~ 0.3	2023-08-30	Version number fix for a neutralization bulletin
~~1.0~~ 1.4	2023-10-19	First remediation version
~~1.1~~ 1.5	2023-11-07	Precision on BullSequana M Adding downfall page Changing minimal TS for BullSequana S (50656) Removing unaffected BullSequana SA references
2.6	2023-11-10	Renumbering to fit with new Eviden template
2.7	2023-12-14	Adding internal reference
2.8	2024-01-19	Updating ETA
2.9	2024-01-26	Correcting ETA
2.10	2024-05-19	Updating ETA for BullSequana M
2.11	2024-07-01	Taking in account BullSequana S TS 74.01 release. Updated ETA for TS 74.01 (Sequana2).

Executive summary

Intel has published a Security Bulletin: INTEL-SA-00828: 2023.3 IPU - Intel® Processor Advisory related to the vulnerability CVE-2022-40982. This bulletin provides a new microcode to mitigate this side channel vulnerability which is affecting several of the BullSequana servers.

The mitigation for this vulnerability may have a severe impact on the processor performance.

Eviden is liaising closely with its suppliers and investigating the exact nature of these vulnerabilities to provide validated remediation. At the time, Eviden do NOT recommend applying microcode updates for Gather Data Sampling (GDS) patching on its HPC nor its Enterprise multi-nodes servers.

Vulnerability Info

Based on our analysis, it is unclear whether the attacker has control over the data it can access through the vulnerability. Depending on cases, the Confidentiality impact could become low, bringing the overall CVSS score to a low level (3.4). Even if Intel recommends its update, the performance impact can become significant on certain vectorization-heavy workloads. Therefore, microcode update is also providing an opt-out mechanism (using bit 4 of the IA32_MCU_OPT_CTRL MSR) which allows system software to disable the mitigation and avoid this drawback.

CVE No.	CVSS Score	Type of Vulnerability
CVE-2022-40982	5.9	CWE-203 - Observable Discrepancy AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C/CR:M/IR:H/AR:H/MAV:L/MAC:L/MPR:L/MUI:N/MS:C/MC:H/MI:N/MA:N

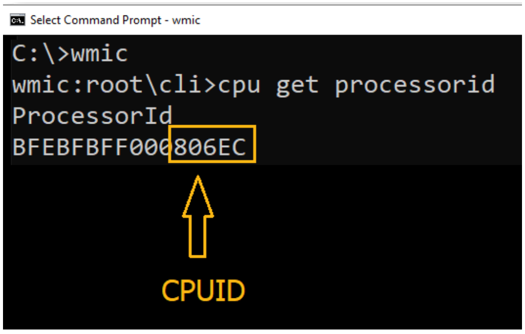
More precisely, the vulnerability lies in the gather instructions used for vectorization to speed up memory accesses to load multiple values from memory operands. Workloads which do not heavily rely on gather instructions are not expected to be impacted by the presence of the GDS microcode mitigation. However, some datacenter and high-performance computing applications, such as machine learning (ML) libraries, numerical libraries, graphic design and rendering software, and certain scientific applications, may see significant performance impact from the GDS microcode mitigation.

Affected products

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.

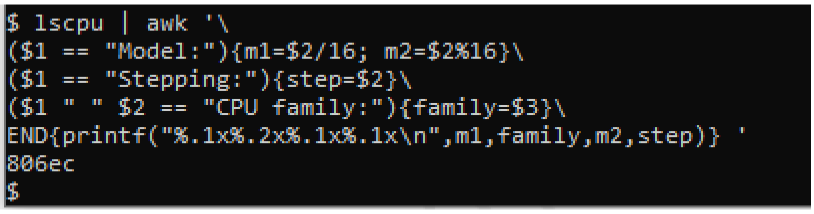


```
C:\>wmic
wmic:root\cli>cpu get processorid
ProcessorId
BFEBFBFF000806EC
```

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	MCU	Comments
Sky Lake	50653	1000181	Stepping B1 Patches as well CVE-2022-21166
Sky Lake	50654	2007006	Stepping H0 Patches as well CVE-2022-21166
Cascade Lake	50655		Stepping A0 Unpatched experimental CPU.
Cascade Lake	50656	04003006	Stepping B0 Patches as well CVE-2022-21166
Cascade Lake	50657	5003604	Stepping B1 Patches as well CVE-2022-21166
Ice Lake Xeon-SP	606A4, 606A5, 606A6	0d0003a5	Patches as well CVE-2022-21233 and CVE-2022-21166
Ice Lake D	606C1	1000211	Patches as well CVE-2022-21233 and CVE-2022-21166

Once determined the CPUID of your server, you can find below the minimal version of Technical State which mitigates CVE-2022-40982. Technical States are available for customers on support.bull.com.

List of Enterprise and Edge servers

The table below provides the Technical State to apply to implement GDS mitigation measures.

CPUID	Bull Sequana S	BullSequana M7200 & M7200V (GCOS7) M9600 (GCOS8)	Bull Sequana E
50653	TS 074.01	TS 074.01	N/A
50654	TS 074.01	TS 074.01	TBD
50655	Unpatched	Unpatched	N/A
50656	TS 064.03	TS 074.01	N/A
50657	TS 074.01	TS 074.01	N/A

List of HPC products

The table below provides the Technical State to apply to implement GDS mitigation measures.

CPUID	Bull Sequana X1120 (CSL) X1125 (CSL-CGP)	Bull Sequana X2135 (CIR)	Bull Sequana X800/QLM (MESCA3)	Bull Sequana X400-E5	Bull Sequana X500-E5
50653	Unpatched	N/A	TS 074.01	TBD	Unpatched
50654	Unpatched	N/A	TS 074.01	TBD	Unpatched
50655	Unpatched	N/A	Unpatched	TBD	Unpatched
50656	Unpatched	N/A	TS 064.03	TBD	Unpatched
50657	Unpatched	N/A	TS 074.01	TBD	Unpatched
606A4, 606A5, 606A6	N/A	TS 074.01 ETA: Q3 2024	N/A	N/A	N/A
606C1	N/A	TS 074.01 ETA: Q3 2024	N/A	N/A	N/A

For X500-E5 platform no patch will be delivered.

Disclaimer

Although Eviden makes effort to provide accurate and complete information, Eviden shall not be liable if the above tables are 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.

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.

Recommendations

Intel recommends that users of affected Intel Processors update to the latest version firmware provided by the system manufacturer that addresses these issues.

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

At the time, Eviden do NOT recommend applying microcode updates for Gather Data Sampling patching on its HPC nor Enterprise servers. See Intel's Threat Analysis of GDS to better assess the risk in your specific context. When validated Technical States will be made available, the GDS mitigation will be turned on by default in the microcode. Operating system vendors (OSVs) may implement options to opt out of the GDS mitigation. Eviden recommends using the OS option to turn off mitigation by default and carefully test the performance impact before activation of the mitigation in production.

Linux systems

RedHat has issued a solution bulletin regarding CVE-2022-40982. The user can disable the mitigation by adding `gather_data_sampling=off` to the kernel command line. Alternatively, to disable all CPU speculative execution mitigations, including GDS, use `mitigations=off`. For instance, this can be done using grub boot loader. Methods to set kernel boot parameters might differ between Linux distributions.

Microsoft systems

For Microsoft operating systems, the bulletin kb5029778 indicates that the opt-out mechanism was not implemented in Windows kernels. Therefore, the application of the mitigation may have a significant impact on performance, with limited rollback possibility.

Available Vendor Patches

Details on how to directly apply microcode updates are provided in Intel's advisory INTEL-SA-00828.html.

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 E	https://support.bull.com/ols/product/platforms/bullion/bullsequana-edge-servers/dl/pkgf/pkgf
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

Usual software mitigation against side channel attacks may mitigate the risks.

Available Exploits/PoC

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

References

1. https://www.intel.com/content/www/us/en/security-center/advisory/INTEL-SA-00828.html
2. https://nvd.nist.gov/vuln/detail/CVE-2022-40982
3. https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/technical-documentation/gather-data-sampling.html
4. https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/processors-affected-consolidated-product-cpu-model.html
5. https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/resources/gds-mitigation-performance-analysis.html
6. https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files
7. https://www.intel.com/content/www/us/en/support/articles/000006831/processors/processor-utilities-and-programs.html
8. https://github.com/intel/Intel-Linux-Processor-Microcode-Data-Files/blob/main/releasenote.md
9. https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=64094e7e3118aff4b0be8ff713c242303e139834
10. https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/best-practices/threat-analysis-gds.html

11. https://access.redhat.com/solutions/7027704
12. https://downfall.page/
13. https://support.bull.com/ols/product/security/psirt/security-bulletins/vulnerabilities-fixed-in-mesca3-psirt-736-tlp-clear-version-2-6-cve-2003-0001-cve-2015-3200-cve-2018-19052-cve-2019-11072-cve-2021-36369-cve-2022-01292-cve-2022-21166-cve-2022-22707-cve-2022-30780-cve-2022-37797-cve-2022-40982-cve-2022-41556-cve-2023/view

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.*