an atos business

Security Bulletin

CacheWrap - AMD Vulnerability in the INVD Instruction

Author(s)	:	Eviden PSIRT
Reference	:	PSIRT-642
Created	:	20 November 2023
Version	:	0.6
Status	:	Neutralization
TLP Classification	:	CLEAR
Document date	:	26 September 2024
Keywords	:	CVE-2023-20592

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	2023/12/17	Initial Neutralization version
0.2	2024/01/26	ETA update
0.3	2024/02/14	Taking in account new TS organization
0.4	2024/06/28	Minor changes
0.5	2024/07/04	BIOS information for Milan updated
0.6	2024/09/26	TLP changed for CLEAR

Executive summary

A potential vulnerability has been identified by external researchers in the INVD instruction, which has the potential to compromise the memory integrity of SEV-ES and SEV-SNP guest virtual machines (VMs).

This security flaw impacts AMD EPYC processors, specifically aimed at the initial generation EPYC Naples, second generation EPYC Rome, and third generation EPYC Milan product lines.

AMD has released an update for third generation EPYC Milan processors in response to the vulnerability discovery. The update includes a microcode patch that can be loaded dynamically and an updated firmware version that aims to fix the issue without affecting system performance. However, AMD has stated that there are no countermeasures available for the Naples and Rome generations of EPYC processors due to the limitations of the SEV and SEV-ES features, which do not safeguard the integrity of guest VM memory, and the absence of SEV-SNP on these older architectures.

Vulnerability Info

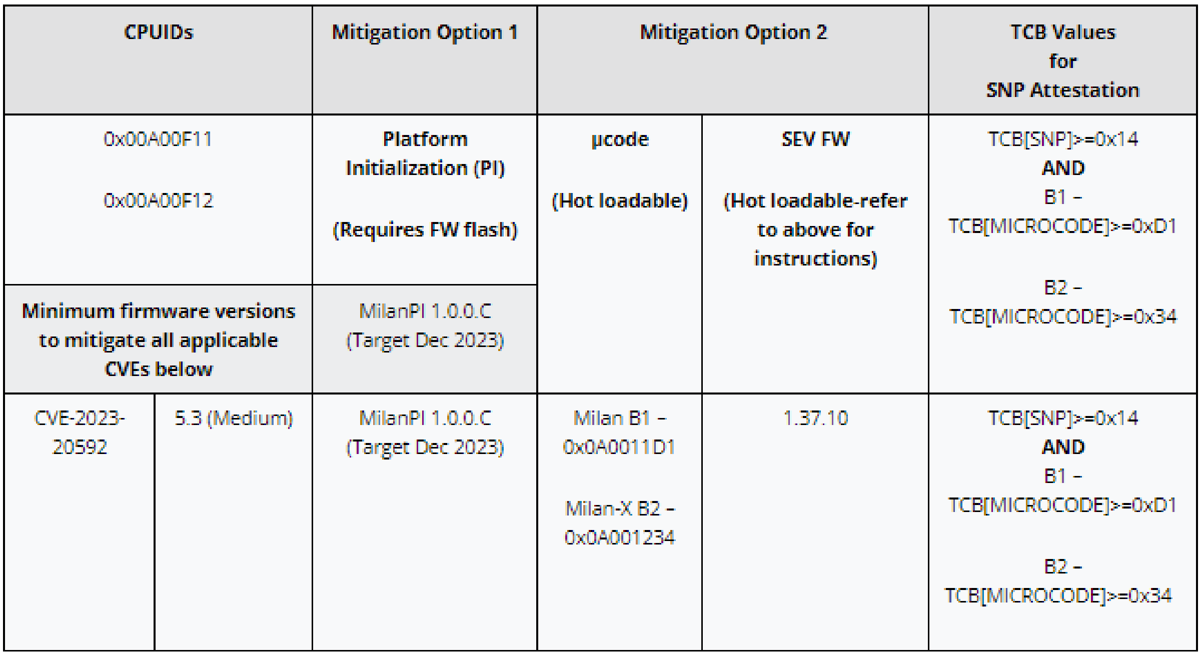
CVE No.	CVSS Score	Type of Vulnerability
CVE-2023-20592	5.3	AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:H/A:N

The weakness in AMD's Secure Encrypted Virtualization (SEV) technology, specifically in the SEV-ES (Encrypted State) and SEV-SNP (Secure Nested Paging) implementations, is exploited by the vulnerability. The CacheWrap attack employs a fault injection technique based on software, which modifies the behavior of cache memory in a virtual machine (VM) that is safeguarded by SEV. By forcing the cache lines within the VM to return to their original state, the attack evades the integrity verification mechanisms of SEV-SNP, enabling undetected fault injection.

CacheWrap poses a systemic threat to any system that relies on AMD's SEV technology, as it exploits inherent architectural weaknesses rather than specific vulnerabilities within the guest VM. This makes it a major concern for ensuring the privacy and integrity of data in environments that rely on encrypted virtualization for security.

Mitigation is not possible for the first and second generations of EPYC™ processors ("Zen 1" or "Naples" and "Zen 2" or "Rome"). This is because the SEV and SEV-ES features are not designed to protect the integrity of guest VM memory.

AMD has taken measures to address the potential vulnerability by offering a hot-loadable microcode patch and updated firmware image for their 3rd generation EPYC™ processors with the SEV-SNP feature enabled. The patch is not expected to have any impact on performance. It should be noted that the 4th generation "Genoa" EPYC™ processors with the "Zen 4" microarchitecture have not been affected by this issue.



CPUIDs		Mitigation Option 1	Mitigation Option 2		TCB Values for SNP Attestation
0x00A00F11 0x00A00F12		**Platform Initialization (PI)** **(Requires FW flash)**	**µcode** **(Hot loadable)**	**SEV FW** **(Hot loadable-refer to above for instructions)**	TCB[SNP]>=0x14 **AND** B1 – TCB[MICROCODE]>=0xD1 B2 – TCB[MICROCODE]>=0x34
Minimum firmware versions to mitigate all applicable CVEs below		MilanPI 1.0.0.C (Target Dec 2023)			
CVE-2023-20592	5.3 (Medium)	MilanPI 1.0.0.C (Target Dec 2023)	Milan B1 – 0x0A0011D1 Milan-X B2 – 0x0A001234	1.37.10	TCB[SNP]>=0x14 **AND** B1 – TCB[MICROCODE]>=0xD1 B2 – TCB[MICROCODE]>=0x34

Affected products

According to AMD risk analysis, the SEV-SNP is the only feature which can be affected in a significant way. Therefore, only Milan CPUs are patched.

The 4th generation of AMD Epyc (Genoa) is unaffected.

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.

List of Enterprise and Edge servers

BullSequana S, SH, and SA1 series are not affected.

CVE	CVSS Score	Bull Sequana SA (Rome)	Bull Sequana SA10 (Milan)	Bull Sequana SA10EL (Milan)	Bull Sequana SA10-NVMe (Milan)
Recommended		**SA0-TSC003**	**SA0-TSC003**	**SA0-TSC003**	**SA0-TSC003**
CVE-2023-20592	5.3	Unpatched	On Request	On Request	On Request

CVE	CVSS Score	Bull Sequana SA20 (Milan)	Bull Sequana SA20-NVMe (Milan)	Bull Sequana SA20G (Milan)	Bull Sequana SA20G-NVMe (Milan)
Recommended		**SA0-TSC003**	**SA0-TSC003**	**SA0-TSC003**	**SA0-TSC003**
CVE-2023-20592	5.3	On Request	On Request	On Request	On Request

List of HPC products

BullSequana X800, X550, X400-A6, X400-E5, XH1000 series are not affected.

BullSequana X400-A5 Series

Products	Fixed version	Status	Remaining vulnerabilities
X410-A5 2U1N1S 4GPU	M12 / MilanPi 1.0.0.A - R26 / RomePI 1.0.0.G	Affected / Unpatched	Rome: CVE-2023-20592 Milan: CVE-2023-20592
X410-A5 2U1N2S 4GPU ALD	M17 / MilanPi 1.0.0.A - R30 / RomePI 1.0.0.G	Affected / Unpatched	
X410-A5 2U1N2S 4GPU SXM	M17 / MilanPi 1.0.0.A - R30 / RomePI 1.0.0.G	Affected / Unpatched	
X410-A5 2U1N2S 8GPU	M15 / MilanPi 1.0.0.A - R22 / RomePI 1.0.0.G	Affected / Unpatched	
X430-A5 2U1N1S	M18 / MilanPi 1.0.0.A - R34 / RomePI 1.0.0.G	Affected / Unpatched	
X430-A5 2U1N2S	M15 / MilanPi 1.0.0.A - R30 / RomePI 1.0.0.G	Affected / Unpatched	
X440-A5 2U4N1S	M14 / MilanPi 1.0.0.A - R28 / RomePI 1.0.0.G	Affected / Unpatched	
X440-A5 2U4N2S	M12 / MilanPi 1.0.0.A - R26 / RomePI 1.0.0.G	Affected / Unpatched	
X450-A5 2U1N2S	M16 / MilanPi 1.0.0.A - R31 / RomePI 1.0.0.G	Affected / Unpatched	

SMS Series

Products	Fixed version	Status	Remaining vulnerabilities
SMC xScale Master / Worker	M18 / MilanPi 1.0.0.A - R34 / RomePI 1.0.0.G	Affected / Unpatched	Rome: CVE-2023-20592 Milan: CVE-2023-20592
SMC Server	M12 / MilanPi 1.0.0.A - R13 / RomePI 1.0.0.G	Affected / Unpatched	

BullSequana XH Series

Products	Fixed version	Status	Remaining vulnerabilities
Bull Sequana XH2410 XH2415 (Rome)	TS68.03 / BIOS_RME090.25.45.001	Unpatched	CVE-2023-20592
Bull Sequana XH2410 XH2415 (Milan)	TS68.03 / BIOS_MLN091.20.30.001	TS ETA: 2024 Q2	CVE-2023-20592

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.

Recommendations

Eviden recommends applying 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.

Technical States links for Eviden servers are reminded in the tables above.

Product	Technical State link
Bull Sequana SA	https://support.bull.com/ols/product/platforms/bullion/bullsequana-sa-servers/dl/pkgf/pkg
Bull Sequana XH2000	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/xh2000/dl/pkgf/pkg
Bull Sequana X400-A5	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400-a5/dl/pkgf/pkg

Available Workarounds

No workaround is available.

Available Mitigations

The CacheWrap attack only applies to virtualized environment.

Available Exploits/PoC

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

References

1. https://cachewarpattack.com/
2. https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3005.html

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.