EVIDEN
an atos business

Security Bulletin

AMI AptioV vulnerabilities - AMI-SA-2023007 and AMI-SA-2023008

Author(s)	:	Eviden PSIRT
Reference	:	PSIRT-673
Created	:	09 November 2023
Version	:	0.7
Status	:	Neutralization
TLP Classification	:	CLEAR
Document date	:	12 June 2025
Keywords	:	CVE-2023-34469 CVE-2023-34470 CVE-2023-39535 CVE-2023-39536 CVE-2023-39537 CVE-2024-2315 CVE-2024-33656 CVE-2024-33657 CVE-2024-33658 CVE-2024-33660 CVE-2024-42442

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	2023/11/09	Initial neutralization version
0.2.	2023/12/22	CVE-2023-39535, CVE-2023-39536, CVE-2023-39537 added to bulletin
0.3	2024/01/29	Link edition.
0.4	2024/04/18	Table with products updated
0.5	2024/08/29	Minor changes and table with version updated, Table for Genoa updated CVE-2024-33657, CVE-2024-33657 added to bulletin
0.6	2025/01/10	CVE-2024-2315,CVE-2024-33658,CVE-2024-33660,CVE-2024-42442 added to bulletin Reverting to TLP:GREEN
0.7	2025/06/12	TLP changed for CLEAR

Executive summary

AMI's PSIRT has taken action in response to a security notification regarding possible vulnerabilities in Aptio V. After conducting a thorough investigation, AMI has verified the presence of two vulnerabilities in Aptio V. These vulnerabilities were discovered by the Binarly efiXplorer Team and were brought to our attention through an external security audit.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2023-34469	4.6	CWE-284 Improper Access Control
CVE-2023-34470	7.8	CWE-284 Improper Access Control
CVE-2023-39535	7.8	CWE-20 Improper Input Validation
CVE-2023-39536	7.8	CWE-20 Improper Input Validation
CVE-2023-39537	7.8	CWE-20 Improper Input Validation
CVE-2024-2315	6.8	CWE-284 Improper Access Control
CVE-2024-33656	7.8	CWE-269 Improper Privilege Management
CVE-2024-33657	7.8	CWE-20 Improper Input Validation
CVE-2024-33658	4.4	CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer
CVE-2024-33660	5.2	CWE-494 Download of Code Without Integrity Check
CVE-2024-42442	7.2	CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

CVE-2023-34469 - score: 4.6

AMI AptioV contains a vulnerability in BIOS where an Attacker may use an improper access control via the physical network. A successful exploit of this vulnerability may lead to a loss of confidentiality.

CVE-2023-34470 - score: 7.8

AMI AptioV contains a vulnerability in BIOS where an Attacker may use an improper access control via the local network. A successful exploit of this vulnerability may lead to a loss of confidentiality, integrity and availability.

CVE-2023-39535, CVE-2023-39536, CVE-2023-39537 - score 7.8

AMI AptioV contains a vulnerability in BIOS where an Attacker may use an improper input validation via the local network. A successful exploit of this vulnerability may lead to a loss of confidentiality, integrity and availability.

CVE-2024-33657 - score 7.8

This SMM vulnerability affects certain modules, allowing privileged attackers to execute arbitrary code, manipulate stack memory, and leak information from SMRAM to kernel space, potentially leading to denial-of-service attacks.

CVE-2024-33656 - score 7.8

The DXE module SmmComputrace contains a vulnerability that allows local attackers to leak stack or global memory. This could lead to privilege escalation, arbitrary code execution, and bypassing OS security mechanisms

CVE-2024-2315 - score 6.8

APTIOV contains a vulnerability in BIOS where may cause Improper Access Control by a local attacker. Successful exploitation of this vulnerability may lead to unexpected SPI flash modifications and BIOS boot kit launches, also impacting the availability.

CVE-2024-33658 - score 4.4

APTIOV contains a vulnerability in BIOS where an attacker may cause an Improper Restriction of Operations within the Bounds of a Memory Buffer by local. Successful exploitation of this vulnerability may lead to privilege escalation and potentially arbitrary code execution, and impact Integrity.

CVE-2024-33660 - score 5.2

An exploit is possible where an actor with physical access can manipulate SPI flash without being detected.

CVE-2024-42442 - score 7.2

APTIOV contains a vulnerability in the BIOS where a user or attacker may cause an improper restriction of operations within the bounds of a memory buffer over the network. A successful exploitation of this vulnerability may lead to code execution outside of the intended System Management Mode.

Affected products

Eviden shall not be liable if the below 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

Rome CPUs

BullSequana SA	Fixed version	Status	Remaining vulnerabilities	BIOS
Recommended	**SA0-TSC003**	**Partially fixed**	**See below.**	
SA10	BIOS R36	TBD	CVE-2023-34470	**Latest (Rome)**
SA10EL	BIOS R36			
SA10-NVMe	BIOS R30			
SA20	BIOS R33a			
SA20-NVMe	BIOS R29			
SA20G	BIOS R32			
SA20G-NVMe	BIOS R29			

Milan CPUs

BullSequana SA	Fixed version	Status	Remaining vulnerabilities	BIOS
Recommended	**SA0-TSC003**	**Partially fixed**	**See below**	
SA10	BIOS M19	TBD	CVE-2023-39536 CVE-2023-39537 CVE-2023-34470	**Latest (Milan)**
SA10EL	BIOS M19			
SA10-NVMe	BIOS M12			
SA20	BIOS M17a			
SA20-NVMe	BIOS M13			
SA20G	BIOS M17			
SA20G-NVMe	BIOS M12			

Genoa CPUs

Products	Fixed version	Status	Remaining vulnerabilities
Recommended	**TS-SA1-0001**	**Partially fixed**	**See below**
SA11a	BIOS F18	TBD	TBD
SA21a	BIOS F21		
SA21Sa	BIOS F21		
SA21Ga	BIOS F12		

List of HPC products

BullSequana 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	TBD	CVE-2023-39536 CVE-2023-39537 CVE-2023-34470
X410-A5 2U1N2S 4GPU ALD	M17 / MilanPi 1.0.0.A - R30 / RomePI 1.0.0.G	TBD	
X410-A5 2U1N2S 4GPU SXM	M17 / MilanPi 1.0.0.A - R30 / RomePI 1.0.0.G	TBD	
X410-A5 2U1N2S 8GPU	M15 / MilanPi 1.0.0.A - R22 / RomePI 1.0.0.G	TBD	
X430-A5 2U1N1S	M18 / MilanPi 1.0.0.A - R34 / RomePI 1.0.0.G	TBD	
X430-A5 2U1N2S	M15 / MilanPi 1.0.0.A - R30 / RomePI 1.0.0.G	TBD	
X440-A5 2U4N1S	M14 / MilanPi 1.0.0.A - R28 / RomePI 1.0.0.G	TBD	
X440-A5 2U4N2S	M12 / MilanPi 1.0.0.A - R26 / RomePI 1.0.0.G	TBD	
X450-A5 2U1N2S	M16 / MilanPi 1.0.0.A - R31 / RomePI 1.0.0.G	TBD	

BullSequana X400-A6 Series

Products	Fixed version	Status	Remaining vulnerabilities
X410-A6 4U1N2S 8G PCIe	F10a / GenoaPI 1.0.0.9	TBD	CVE-2023-34470
X430-A6 2U1N1s	F10a / GenoaPI 1.0.0.8	TBD	
X430-A6 2U1N2S	F13a / GenoaPI 1.0.0.9	TBD	
X440-A6 2U4N2S	F10a/ GenoaPI 1.0.0.9	TBD	
X450-A6 2U1N2S 2G	F13a / GenoaPI 1.0.0.9	TBD	

BullSequana X400-E7 Series

Products	Fixed version	Status	Remaining vulnerabilities
X410-E7 4U1N2S 8G PCIe	TBD	TBD	TBD
X430-E7 2U1N1S	R03	TBD	
X430-E7 2U1N2S	R04	TBD	
X440-E7 2U4N2S	R04	TBD	
X450-E7 2U1N2S 2G	R03	TBD	
X450-E7 2U1N2S 4G	R04	TBD	

BullSequana XH Series

Products	Fixed version	Status	Remaining vulnerabilities
Bull Sequana XH2410 XH2415 (Rome)	TBD	TBD	CVE-2023-39536 CVE-2023-39537 CVE-2023-34470
Bull Sequana XH2410 XH2415 (Milan)	TBD	TBD	CVE-2023-39536 CVE-2023-39537 CVE-2023-34470
Bull Sequana XH3420 XH3406 (Genoa)	TBD	TBD	CVE-2023-34470

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.

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 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 the reported vulnerabilities.

References

1. https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023007.pdf
2. https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023008.pdf
3. https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/2024/AMI-SA-2024004.pdf

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.