EVIDEN
an atos business

Security Bulletin

AMI MegaRAC BMC Multiple Vulnerabilities

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-513**
Created	:	**19 December 2022**
Version	:	**2.14**
Status	:	**Remediation**
TLP Classification	:	**CLEAR**
Document date	:	**12 June 2025**
Keywords	:	**CVE-2022-02827 CVE-2022-26872 CVE-2022-40242 CVE-2022-40258 CVE-2022-40259 CVE-2023-02975 CVE-2023-03043 CVE-2023-3708 CVE-2023-05678 CVE-2023-06606 CVE-2023-25191 CVE-2023-25192 CVE-2023-28863 CVE-2023-31085 CVE-2023-31130 CVE-2023-34329 CVE-2023-34330 CVE-2023-34332 CVE-2023-34333 CVE-2023-34334 CVE-2023-34335 CVE-2023-34336 CVE-2023-34337 CVE-2023-34338 CVE-2023-34341 CVE-2023-34342 CVE-2023-34343 CVE-2023-34344 CVE-2023-34345 CVE-2023-34471 CVE-2023-34472 CVE-2023-34473 CVE-2023-37293 CVE-2023-37294 CVE-2023-37295 CVE-2023-37296 CVE-2023-37297 CVE-2023-46218 CVE-2023-48795**

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	2022-19-12	Neutralization
1.0 1.2	2023-01-02	Remediation
1.1 1.3	2023-01-09	Remediation
1.2 1.4	2023-01-12	Remediation
1.3 1.5	2023-03-10	Remediation
0.6	2023-11-11	Renumbering to fit with the new Eviden template. Back to neutralization state given the results of internal investigation on additional vulnerabilities
1.7	2023-11-12	Remediation for HPC
1.8	2023-11-12	Remediation for HEP
1.9	2023-12-17	Internal PSIRT reference. Introducing CMC 12.41.32 version
1.10	2024-01-26	TLP changed for visibility of patches.
1.11	2024-03-07	Major update to take in account latest bulletins from AMI and GigaByte. Added CVE-2023-03043, CVE-2023-34332, CVE-2023-34333, CVE-2023-37293, CVE-2023-37294, CVE-2023-37295, CVE-2023-37296, CVE-2023-37297 Take in account latests TS for all platforms.
1.12	2024-04-26	Minor modification after internal review. Waiting for supplier statements.
1.13	2024/12/24	CVE-2024-3708 added to bulletin. Reference added to bulletin, other vulnerabilities added (Gigabyte publication)
2.14	2025/06/12	TLP changed for CLEAR

Executive summary

In August 2022, Eclypsium Research was made aware of a leak of intellectual property, purported to come from AMI, which had been posted online. After downloading and reviewing the data, it appeared legitimate, and since there was a chance others had accessed it the decision was made to look for vulnerabilities in case malicious actors were doing the same. The focus quickly narrowed down to the Redfish API, as it is remotely accessible and a first choice for attackers.

On December 7, 2022, three vulnerabilities have been reported by American Megatrends Inc.'s MegaRAC Baseboard Management Controller (BMC) software: CVE-2022-40259, CVE-2022-40242, and CVE-2022-2827.

These vulnerabilities can pose a serious risk of supply chain attacks. Multiple server providers, including Gigabyte, NVidia, AMD, Asus, Huawei, Lenovo, Quanta, and Dell EMC, use MegaRAC BMC.

MegaRAC BMC firmware is one of the common threads that connects much of the hardware that underlies the cloud. As a result, any vulnerability in MegaRAC can easily spread through the extended supply chain to affect dozens of vendors and potentially millions of servers

On January 30, 2023 two new vulnerabilities have been reported by American Megatrends Inc.'s MegaRAC Baseboard Management Controller (BMC) software: CVE-2022-26872, CVE-2022-40258.

In June 2023, AMI issued a new security bulletin with 9 vulnerabilities ranging from 5.3 (Medium) to 8.1 (High) CVSS score.

Again, on July 20, 2023, two new vulnerabilities CVE-2023-34329 and CVE-2023-34330 were published by Eclypsium Research. These new vulnerabilities range in severity from High to Critical, including *unauthenticated* **remote code execution and unauthorized device access with superuser permissions**. They can be exploited by any local or remote attacker having access to the Redfish management interface.

Given the recurrence of the publication of new vulnerabilities, Eviden liaised closely with its suppliers to investigate these vulnerabilities and provide validated remediation. In this process, it was identified that the presumably fixed older vulnerabilities had not been patched properly. It is therefore even more recommended to update the firmware of the affected products.

On April 15, 2024 one new vulnerability has been reported by American Megatrends Inc.'s MegaRAC Baseboard Management Controller (BMC) software: CVE-2024-3708.

Vulnerability Info

Given the unusual number of vulnerabilities, we have removed the description of each of them. Please refer to the references section should you want to have further details on them.

Global risk analysis

When these vulnerabilities are chained together, even a remote attacker with network access to BMC management interface and no BMC credentials, can

achieve remote code execution by tricking BMC into believing that the http request is coming from the internal interface. As a result, the attacker can remotely upload and execute arbitrary code, possibly from the Internet, if the BMC interface is exposed to it.

The impact of exploiting these vulnerabilities includes remote control of compromised servers, remote deployment of malware, ransomware and firmware implanting or bricking motherboard components (BMC or potentially BIOS/UEFI), potential physical damage (over-voltage / bricking), and indefinite reboot loops that a victim cannot easily stop.

CVE	CVSS Score	AMI Bulletin	Giga Computing Bulletin
CVE-2022-02827	7.5	AMI-SA-2023001	2044
CVE-2022-26872	8.8	AMI-SA-2023001	2151
CVE-2022-40242	9.8	AMI-SA-2023001	2044
CVE-2022-40258	5.3	AMI-SA-2023001	2151
CVE-2022-40259	9.8	AMI-SA-2023001	2044
CVE-2023-2975	5.3		2217
CVE-2023-03043	9.6	AMI-SA-2023010	2217
CVE-2023-5678	5.3		2217
CVE-2023-6606	7.1		2217
CVE-2023-25191	7.5	AMI-SA-2023005	
CVE-2023-25192	5.3	AMI-SA-2023002	
CVE-2023-28863	5.9	AMI-SA-2023003	2151
CVE-2023-31085	5.5		2217
CVE-2023-31130	6.4		2217
CVE-2023-34329	9.1	AMI-SA-2023006	2102
CVE-2023-34330	8.2	AMI-SA-2023006	2102
CVE-2023-34332	7.8	AMI-SA-2023010	
CVE-2023-34333	7.8	AMI-SA-2023010	
CVE-2023-34334	8.8	AMI-SA-2023005	
CVE-2023-34335	9.1	AMI-SA-2023005	
CVE-2023-34336	8.8	AMI-SA-2023005	
CVE-2023-34337	7.6	AMI-SA-2023006	2151
CVE-2023-34338	7.1	AMI-SA-2023006	2151
CVE-2023-34341	8.8	AMI-SA-2023005	
CVE-2023-34342	9.1	AMI-SA-2023005	

CVE	CVSS Score	AMI Bulletin	Giga Computing Bulletin
CVE-2023-34343	8.8	AMI-SA-2023005	
CVE-2023-34344	5.3	AMI-SA-2023005	
CVE-2023-34345	6.5	AMI-SA-2023005	
CVE-2023-34471	6.3	AMI-SA-2023006	2151
CVE-2023-34472	5.7	AMI-SA-2023006	2151
CVE-2023-34473	6.6	AMI-SA-2023006	2151
CVE-2023-37293	9.6	AMI-SA-2023010	
CVE-2023-37294	8.3	AMI-SA-2023010	
CVE-2023-37295	8.3	AMI-SA-2023010	
CVE-2023-37296	8.3	AMI-SA-2023010	
CVE-2023-37297	8.3	AMI-SA-2023010	
CVE-2023-46218	6.5		2217
CVE-2023-48795	5.9		2217
CVE-2024-3708	5.7	AMI-SA-2024002	

Affected products

List of Enterprise and Edge servers

BullSequana S, M, E, SH, MH, and EH series are not affected.

The table below provides the Technical State to apply to implement the AMI fixes on Eviden products.

Note: The first row provides the current recommended combination of firmware. The detail per vulnerability is given below.

Rome and Milan CPUs

Products	Fixed version	Status	Remaining vulnerabilities
Recommended	**SA0-TSC003**	**Partially fixed**	**See below.**
Bull Sequana SA10	BMC 12.61.19	Partially fixed	CVE-2023-25191, CVE-2023-25192, CVE-2023-34334, CVE-2023-34336, CVE-2023-34341, CVE-2023-34342, CVE-2023-34343, CVE-2023-34344, CVE-2023-34345
Bull Sequana SA10EL			
Bull Sequana SA10-NVMe			
Bull Sequana SA20			
Bull Sequana SA20-NVMe			
Bull Sequana SA20G			
Bull Sequana SA20G-NVMe			

Genoa CPUs

Products	Fixed version	Status	Remaining vulnerabilities
Recommended	**TS-SA1-0001**	**Partially fixed**	**See below**
Bull Sequana SA11a	BMC 13.05.01	Partially Fixed	All vulnerabilities but: CVE-2022-40242
Bull Sequana SA21a			
Bull Sequana SA21Sa			

List of HPC products

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

The table below provides the Technical State to apply to implement the AMI fixes on Eviden products.

Note: The first row provides the current recommended combination of firmware. The detail per vulnerability is given below. The Bull Sequana X440-A5/A6/E7 needs both BMC and CMC upgrades.

BullSequana X400-A5 Series

Products	Fixed version	Status	Remaining vulnerabilities
X410-A5 2U1N1S 4GPU X410-A5 2U1N2S 8GPU X430-A5 2U1N1S X430-A5 2U1N2S X450-A5 2U1N2S	BMC 12.61.17	Partially Fixed	CVE-2023-25191, CVE-2023-25192, CVE-2023-34334, CVE-2023-34336, CVE-2023-34341, CVE-2023-34342, CVE-2023-34343, CVE-2023-34344, CVE-2023-34345
X440-A5 2U4N1S X440-A5 2U4N2S	BMC 12.61.17 CMC 12.41.32	Partially Fixed	BMC: see above CMC: CVE-2023-03043, CVE-2023-25192, CVE-2023-34342, CVE-2023-34344, CVE-2023-34345, CVE-2023-37293, CVE-2023-37294, CVE-2023-37295, CVE-2023-37296, CVE-2023-37297
X410-A5 2U1N2S 4GPU ALD X410-A5 2U1N2S 4GPU SXM	BMC 12.83.48	Partially Fixed	CVE-2022-02827, CVE-2022-40259, CVE-2023-25191, CVE-2023-25192, CVE-2023-34334, CVE-2023-34336, CVE-2023-34341, CVE-2023-34342, CVE-2023-34343, CVE-2023-34344, CVE-2023-34345

SMS Series

Products	Fixed version	Status	Remaining vulnerabilities
SMC xScale Master / Worker SMC Server	BMC 12.61.17	Partially Fixed	CVE-2023-25191, CVE-2023-25192, CVE-2023-34334, CVE-2023-34336, CVE-2023-34341, CVE-2023-34342, CVE-2023-34343, CVE-2023-34344, CVE-2023-34345

BullSequana X400-A6 Series

Products	Fixed version	Status	Remaining vulnerabilities
X410-A6 4U1N2S 8G PCIe	BMC 13.05.07	Partially Fixed	CVE-2023-25191, CVE-2023-25192, CVE-2023-34334, CVE-2023-34335, CVE-2023-34336, CVE-2023-34341, CVE-2023-34342, CVE-2023-34343, CVE-2023-34344, CVE-2023-34345 CVE-2023-3043, CVE-2023-2975, CVE-2023-5678, CVE-2023-31085, CVE-2023-6606, CVE-2023-31130, CVE-2023-48795, CVE-2023-46218
X430-A6 2U1N1s			
X430-A6 2U1N2S			
X450-A6 2U1N2S 2G	BMC 13.06.07		

X440-A6 2U4N2S	BMC 13.05.07 CMC 12.41.32	Partially Fixed	BMC: see above CMC: CVE-2023-03043, CVE-2023-25192, CVE-2023-34342, CVE-2023-34344, CVE-2023-34345, CVE-2023-37293, CVE-2023-37294, CVE-2023-37295, CVE-2023-37296,

BullSequana X400-E7 Series

Products	Fixed version	Status	Remaining vulnerabilities
X430-E7 2U1N1s X430-E7 2U1N2S X450-E7 2U1N2S 2G	BMC 13.05.07	Partially Fixed	CVE-2023-25191, CVE-2023-25192, CVE-2023-34334, CVE-2023-34335, CVE-2023-34336, CVE-2023-34341, CVE-2023-34342, CVE-2023-34343, CVE-2023-34344, CVE-2023-34345
X440-E7 2U4N2S	BMC 13.05.07 CMC 12.41.32	Partially Fixed	BMC: see above CMC: CVE-2023-03043, CVE-2023-25192, CVE-2023-34342, CVE-2023-34344, CVE-2023-34345, CVE-2023-37293, CVE-2023-37294, CVE-2023-37295, CVE-2023-37296,

BullSequana XH Series

Products	Fixed version	Status	Remaining vulnerabilities
Bull Sequana XH2410 XH2415	TS68.05 EMM60 60.99.0.0	Partially Fixed	All but: CVE-2022-2827 CVE-2022-40242 CVE-2022-40259 CVE-2023-34329
Bull Sequana XH3420 (Genoa)	TS04.02 BMC_GEN.13.90.24	Partially Affected	All but: CVE-2022-2827 CVE-2022-40242

TS (technical state) indicates that a new technical state fixing the vulnerabilities is scheduled for delivery.

TBD (to be defined) indicates that a new technical state fixing the vulnerabilities is under study. Older systems will be investigated on demand.

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

Available Vendor Patches

Eviden is working with its suppliers to distribute updates as soon as possible as described above.

Server manufacturers that are known to have used MegaRAC BMC include but are not limited to the following: AMD, Ampere Computing, ASRock, Asus, ARM, Dell EMC, Gigabyte, Hewlett-Packard Enterprise, Huawei, Inspur, Lenovo, Nvidia, Qualcomm, Quanta.

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

Ensure that all remote server management interfaces (e.g. Redfish, IPMI) and BMC subsystems in their environments are on their dedicated management networks and are not exposed externally, and ensure internal BMC interface access is restricted to administrative users with ACLs or firewalls.

Available Exploits/PoC

Eviden is not aware of any exploitation of the reported vulnerabilities on its products.

There is no information or evidence that the vulnerabilities are actively exploited but exploiting these vulnerabilities could lead to physical damage to the server, remotely malware deployment, ransomware infection or remote control attacked servers.

These vulnerabilities can be exploited by an attacker who accessed the data center or administrative network. Any security vulnerability at the BMC level can impact a significant number of devices and could potentially affect the entire data center and the services it offers.

Because standard EDR and AV products focus on the operating system rather than the firmware, exploitation of BMC vulnerabilities is difficult to detect due to their location and nature.

References

1. https://www.gigabyte.com/Support/Security/2044
2. https://www.gigabyte.com/fr/Support/Security/2102
3. https://eclypsium.com/2022/12/05/supply-chain-vulnerabilities-put-server-ecosystem-at-risk/
4. https://eclypsium.com/research/bmcc-lights-out-forever/
5. https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023001.pdf
6. https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023005.pdf
7. https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023006.pdf
8. https://security.netapp.com/advisory/ntap-20230814-0004/
9. https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/2024/AMI-SA-2024002.pdf
10. https://www.gigabyte.com/fr/Support/Security/2217

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.