EVIDEN
an atos business

Security Bulletin

Major Vulnerabilities in Supermicro BMCs

Author(s)	:	Eviden PSIRT
Reference	:	PSIRT-1019
Created	:	18 January 2024
Version	:	0.5
Status	:	Neutralization
TLP Classification	:	CLEAR
Document date	:	3 July 2025
Keywords	:	CVE-2023-33411, CVE-2023-33412, CVE-2023-33413 CVE-2023-40284, CVE-2023-40285, CVE-2023-40286, CVE-2023-40287, CVE-2023-40288, CVE-2023-40289, CVE-2023-40290 CVE-2024-36435

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	2024/02/02	Initial Neutralization version
0.2	2024/07/11	CVE-2024-36435 added to bulletin, title changed.
0.3	2024/10/03	Minor changes (waiting for TS), BRLY-2024-023 added to bulletin. Reference added
0.4	2025/02/03	Changed status for Unpatched
0.5	2025/07/03	TLP changed for CLEAR

Executive summary

Researchers from security firm Binarly disclosed seven high-severity vulnerabilities in the IPMI (Intelligent Platform Management Interface) firmware for older Supermicro Baseboard Management controllers (BMCs). According to Supermicro the vulnerabilities affect "select X11, H11, B11, CMM, M11, and H12 motherboards." Supermicro said it's unaware of any malicious exploitation of the vulnerabilities in the wild.

The bulletin also contains vulnerabilities for which: A web server in the Intelligent Platform Management Interface (IPMI) baseboard management controller (BMC) implementation on Supermicro X11 and M11 based devices, with firmware versions up to 3.17.02, allows remote unauthenticated users to perform directory traversal, potentially disclosing sensitive information.

Supermicro reported potential vulnerability in Supermicro BMC may come from a buffer overflow in the “GetValue” function of the firmware that is caused by a lack of checking the input value. An unauthenticated user can post specially crafted data to the interface, which will trigger a stack buffer overflow and may lead to arbitrary remote code execution on a BMC. - CVE-2024-36435

Eviden is liaising closely with its suppliers and investigating the exact nature of these vulnerabilities to provide validated remediation.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2023-40289	7.2	CWE-78: Improper Neutralization of Special Elements used in an OS Command AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
CVE-2023-40284	8.3	CWE-79: Improper Neutralization of Input During Web Page Generation AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
CVE-2023-40287	8.3	CWE-79: Improper Neutralization of Input During Web Page Generation

		AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
CVE-2023-40288	8.3	CWE-79: Improper Neutralization of Input During Web Page Generation AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
CVE-2023-40290	8.3	CWE-79: Improper Neutralization of Input During Web Page Generation AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
CVE-2023-40285	8.3	CWE-79: Improper Neutralization of Input During Web Page Generation AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
CVE-2023-40286	8.3	CWE-79: Improper Neutralization of Input During Web Page Generation AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
CVE-2023-33411	7.5	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVE-2023-33412	8.8	Insufficient Information AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2023-33413	8.8	CWE-798: Use of Hard-coded Credentials AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2024-36435	9.8	CWE-121 Stack-based Buffer Overflow AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
brly-2024-023	9.1	TBD

CVE-2023-40289
An attacker needs to be logged into BMC with administrator privileges to exploit the vulnerability. An unvalidated input value could allow the attacker to perform command injection.

CVE-2023-40284, CVE-2023-40287, CVE-2023-40288
An attacker could send a phishing link that does not require login, tricking BMC administrators to click on that link while they are still logged in and thus authenticated by BMC Web UI.

CVE-2023-40290
An attacker could send a phishing link that does not require login, tricking BMC administrators to click on that link while they are still logged in and thus authenticated by BMC Web UI. This vulnerability can only be exploited using Windows IE11 browser.

CVE-2023-40285
An attacker could send a phishing link that does not require login, tricking BMC administrators to click on that link while they are still logged in and thus authenticated by BMC Web UI. The attacker poisons the administrator's browser cookies to create a new user.

CVE-2023-40286
An attacker could send a phishing link that does not require login, tricking BMC administrators to click on that link while they are still logged in and thus authenticated by BMC Web UI. The attacker poisons the administrator's browser cookies and local storage to create a new user.

CVE-2023-33411
IPMI BMC SSDP/UPnP web server directory traversal and iKVM access allowing the rebooting of the host

CVE-2023-33412
IPMI BMC administrative web interface virtual floppy/USB remote command execution

CVE-2023-33413
IPMI BMC devices use hardcoded configuration file encryption keys, allowing the attacker to craft and upload a malicious configuration file packages to gain remote command execution

CVE-2024-36435
This potential vulnerability in Supermicro BMC may come from a buffer overflow in the "GetValue" function of the firmware that is caused by a lack of checking the input value.An unauthenticated user can post specially crafted data to the interface, which will trigger a stack buffer overflow and may lead to arbitrary remote code execution on a BMC.

BRLY-2024-023

The BINARLY team has discovered that multiple Supermicro servers use an insecure RSA signing key (RD1 BMC Test Key - DO NOT TRUST) to implement the BMC Root of Trust security feature. The use of test keys poses a critical severity risk by making it trivial for remote attackers with administrative privileges to the BMC system to perform a malicious BMC firmware update and defeat U-Boot verified boot on affected devices. This results in a persistent compromise of both the BMC system and the main server operating system.

Affected products

Products	Fixed version	Status	Comments
Bull Sequana X400-E5	Unpatched	Affected	
Bull Sequana X500-E5	Unpatched	Affected	
Bullx R400-E4	Unpatched	Affected	

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.

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 HPC products

CVE	CVSS Score	Bull Sequana X400-E5	Bull Sequana X500-E5	Bullx R400-E4
Recommended		**TBD**	**TBD**	**TBD**
CVE-2023-40289	7.2	TBD	TBD	TBD
CVE-2023-40284	8.3	TBD	TBD	TBD
CVE-2023-40287	8.3	TBD	TBD	TBD
CVE-2023-40288	8.3	TBD	TBD	TBD

CVE	CVSS Score	Bull Sequana X400-E5	Bull Sequana X500-E5	Bullx R400-E4
CVE-2023-40290	8.3	TBD	TBD	TBD
CVE-2023-40285	8.3	TBD	TBD	TBD
CVE-2023-40286	8.3	TBD	TBD	TBD
CVE-2023-33411	7.5	TBD	TBD	TBD
CVE-2023-33412	8.8	TBD	TBD	TBD
CVE-2023-33413	8.8	TBD	TBD	TBD
CVE-2024-36435	9.8	TBD	TBD	TBD
BRLY-2024-023	9.1	TBD	TBD	TBD

Recommendations

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

Affected Supermicro motherboard SKUs will require a BMC update to mitigate these potential vulnerabilities. It is advised to follow the BMC Configuration Best Practices Guide and configure session timeout.

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 X400-E5	https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkg

Available Workarounds

As an immediate workaround to reduce the attack surface, it is advised to follow the BMC Configuration Best Practices Guide [link] and configure session timeout.

Available Mitigations

BMCs are usually connected to management networks which are not exposed to the Internet.

Available Exploits/PoC

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

References

1. https://www.supermicro.com/en/support/security_BMC_IPMI_Oct_2023
2. https://www.supermicro.com/products/nfo/files/IPMI/Best_Practices_BMC_Security.pdf
3. https://binarly.io/posts/Binarly_REsearch_Uncovers_Major_Vulnerabilities_in_Supermicro_BMCs/index.html
4. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3426648/nsa-and-cisa-release-guide-to-protect-baseboard-management-controllers/
5. https://www.binarly.io/blog/cve-2024-36435-deep-dive-the-years-most-critical-bmc-security-flaw

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.