EVIDEN
an atos business

Security Bulletin

Vulnerabilities in Insyde H2O BIOS

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-697**
Created	:	**07 June 2024**
Version	:	**0.7**
Status	:	**Neutralization**
TLP Classification	:	**CLEAR**
Document date	:	**12 June 2025**
Keywords	:	**CVE-2020-5952 CVE-2023-27471 CVE-2023-28149 CVE-2023-30633 CVE-2023-31041 CVE-2023-39284 CVE-2023-47252 CVE-2024-25078 CVE-2024-25079 CVE-2024-27353 CVE-2024-39707**

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	2024/03/19	Initial neutralization version
0.2	2024/03/23	Minor changes in title site. Removing BullSequana SA and X400 series from the list of affected products.
0.3	2024/05/19	CVE-2023-47252, CVE-2024-25078, CVE-2024-25079, CVE-2024-27353 added to bulletin
0.4	2024/05/24	CVE-2020-5952, CVE-2023-28149 added to bulletin
0.5	2024/06/14	Minor changes
0.6	2025/01/09	CVE-2024-39707 added to bulletin
0.7	2025/06/12	TLP changed for CLEAR, fix versions have been changed for Unpatched stasus

Executive summary

Insyde published Security Advisories 2023036, 2023047, 2023045, 2023067, 2024007 with vulnerabilities affecting InsydeH2O BIOS. Vulnerabilities occur with scores from 4.1 to 6.1.

Vulnerable components are embedded in BullSequana X, S, M and SH series.

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-2020-5952	7.2	TBD
CVE-2023-27471	5.5	TBD
CVE-2023-28149	6.1	TBD
CVE-2023-30633	5.3	TBD
CVE-2023-31041	7.5	CWE-312 Cleartext Storage of Sensitive Information
CVE-2023-39284	5.5	TBD
CVE-2023-47252	4.7	TBD
CVE-2024-25078	7.4	TBD
CVE-2024-25079	7.4	TBD
CVE-2024-27353	7.4	TBD
CVE-2024-39707	5.3	CWE-306 Missing Authentication for Critical Function

CVE-2023-27471

An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. UEFI

implementations do not correctly protect and validate information contained in the 'MeSetup' UEFI variable. On some systems, this variable can be overwritten using operating system APIs. Exploitation of this vulnerability could potentially lead to denial of service for the platform.

CVE-2023-30633
An issue was discovered in TrEEConfigDriver in Insyde InsydeH2O with kernel 5.0 through 5.5. It can report false TPM PCR values, and thus mask malware activity. Devices use Platform Configuration Registers (PCRs) to record information about device and software configuration to ensure that the boot process is secure. (For example, Windows uses these PCR measurements to determine device health.) A vulnerable device can masquerade as a healthy device by extending arbitrary values into Platform Configuration Register (PCR) banks. This requires physical access to a target victim's device, or compromise of user credentials for a device.

CVE-2023-31041
An issue was discovered in SysPasswordDxe in Insyde InsydeH2O with kernel 5.0 through 5.5. System password information could optionally be stored in cleartext, which might lead to possible information disclosure.

CVE-2023-39284

SMI handler that passes attacker controlled arguments to SmmSetVariable() without any sort of filtering/sanitization.

CVE-2023-47252

An issue was discovered in PnpSmm in Insyde InsydeH2O with kernel 5.0 through 5.6. There is a possible out-of-bounds access in the SMM communication buffer, leading to tampering. The PNP-related SMI sub-functions do not verify data size before getting it from the communication buffer, which could lead to possible circumstances where the data immediately following the command buffer could be destroyed with a fixed value. This is fixed in kernel 5.2 v05.28.45, kernel 5.3 v05.37.45, kernel 5.4 v05.45.45, kernel 5.5 v05.53.45, and kernel 5.6 v05.60.45.

CVE-2024-25078

StorageSecurityCommandDxe: SMM memory corruption vulnerability could lead to escalating privileges in SMM.

CVE-2024-25079

HddPassword: SMM memory corruption vulnerability could lead to escalating privileges to SMM.

CVE-2024-27353

SdHost / SdMmcDevice: SMM memory corruption vulnerability could lead to escalating privileges in SMM.

CVE-2020-5952

AhciBusDxe module has an SMM call out vulnerability that could also be used to execute arbitrary code at SMM level.

CVE-2023-28149

A vulnerability in the IhisiServiceSmm module that could allow an attacker to modify UEFI variables.

CVE-2024-39707

IHISI function 0x49 can restore factory defaults for certain UEFI variables without further authentication by default, which could lead to a possible roll-back attack in certain platforms.

This has the same root cause as CVE-2023-28149 but with different impact.

Affected products

Atos BIOS

Products	Fixed version	Status	Comments
Bakerville	TBD	Affected	Not affected by CVE-2023-27471
Eaglestream	TBD	Affected	
Idaville	TBD	Affected	
Purleyclxserver	TBD	Affected	
Whitleyclxcpxicx	TBD	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 Enterprise and Edge servers

BullSequana SA servers are not affected.

CVE	CVSS Score	Bull Sequana M	Bull Sequana S	Bull Sequana SH	Bull Sequana Edge
Recommended		Unpatched	Unpatched	Unpatched	Unpatched
CVE-2020-5952	7.2	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2023-27471	5.5	Not affected	Not affected	Not affected	Not affected
CVE-2023-28149	6.1	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2023-30633	5.3	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2023-31041	7.5	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2023-39284	5.5	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2023-47252	4.7	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2024-25078	7.4	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2024-25079	7.4	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2024-27353	7.4	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2024-39707	5.3	Unpatched	Unpatched	Unpatched	Unpatched

List of HPC products

BullSequana X4OO and X500 series are not affected.

CVE	CVSS Score	Bull Sequana X80x X816 QLM	Bull Sequana X1120 X1122	Bull Sequana XH2135 XH2140	Bull Sequana XH3140
Recommended		Unpatched	Unpatched	Unpatched	Unpatched
CVE-2020-5952	7.2	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2023-27471	5.5	Not affected	Not affected	Not affected	Not affected
CVE-2023-28149	6.1	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2023-30633	5.3	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2023-31041	7.5	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2023-39284	5.5	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2023-47252	4.7	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2024-25078	7.4	Unpatched	Unpatched	Unpatched	Unpatched

CVE-2024-25079	7.4	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2024-27353	7.4	Unpatched	Unpatched	Unpatched	Unpatched
CVE-2024-39707	5.3	Unpatched	Unpatched	Unpatched	Unpatched

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 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 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://www.insyde.com/security-pledge
2. https://www.insyde.com/security-pledge/SA-2023036
3. https://www.insyde.com/security-pledge/SA-2023045
4. https://www.insyde.com/security-pledge/SA-2023047
5. https://www.insyde.com/security-pledge/SA-2023067
6. https://www.insyde.com/security-pledge/SA-2024001
7. https://nvd.nist.gov/vuln/detail/CVE-2023-27471
8. https://nvd.nist.gov/vuln/detail/CVE-2023-30633
9. https://nvd.nist.gov/vuln/detail/CVE-2023-31041
10. https://nvd.nist.gov/vuln/detail/CVE-2023-47252
11. https://nvd.nist.gov/vuln/detail/CVE-2024-25078
12. https://nvd.nist.gov/vuln/detail/CVE-2024-25079
13. https://nvd.nist.gov/vuln/detail/CVE-2024-27353
14. https://nvd.nist.gov/vuln/detail/CVE-2020-5952
15. https://www.insyde.com/security-pledge/SA-2020001
16.

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.