Security Bulletin:

UEFI vulnerabilities affecting BullSequana servers VU#796611

Author : Atos BDS TI Team
Created : 2022-02-02
Last Update : 2022-05-30
Revision : 2.0
Keywords :

TLP:WHITE

Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Executive summary

On February 1st, 2022, CERT-CC, Insyde Inc., and Binarly Inc. collectively disclosed a set of vulnerabilities affecting InsydeH2O Hardware-2-Operating System (H2O) UEFI Bios.

These vulnerabilities generalize to all Intel and AMD chipset configurations a 2020 vulnerability affecting a version of InsydeH2O that supported a specific Intel chipset (CVE-2020-5953). They affect any product using UEFI Bios based on InsydeH2O, including some BullSequana products.

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

Vulnerability Info

The management part of the platforms (BMC) is not affected by these vulnerabilities. The vulnerability lies in the computing part of the servers.

An administrative access to the host would allow to implement hardly detectable malware in the System Management Mode (SMM) area. Under certain circumstances, these vulnerabilities could help to circumvent secure boot and other security features which preserve the integrity of the platform firmware.

CVE No.	CVSS Score	Type of Vulnerability
CVE-2020-5953 CVE-2021-33625 CVE-2021-42060 CVE-2021-42113 CVE-2021-42554 CVE-2021-43323 CVE-2021-43522 CVE-2021-43615 CVE-2022-24030 CVE-2022-24031 CVE-2022-24069	7.8 AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:F/RL:U/RC:C	Multiple vulnerabilities in SMM (System Management Mode) can lead to escalation of privileges reserved only for SMM with persistence across reboot.
CVE-2021-42059	6.5 AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C	Stack overflow vulnerability that allows a local root user to access UEFI DXE driver and execute arbitrary code.
CVE-2021-45969 CVE-2021-45970 CVE-2021-45971	7.8 AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:F/RL:U/RC:C	Multiple vulnerabilities in SMRAM management can lead to arbitrary code execution in SMM with persistence across reboot.

Affected products

HPC	Fixed Version	Status	Comments
Atos QLM	TS 54.01	Affected	ETA: March 31st
Bullx S6010 Bullx S6030 Bullx S6130	TBD	Affected	
Bull Sequana X802 Bull Sequana X804 Bull Sequana X808 Bull Sequana X816	TS 54.01	Affected	ETA: March 31st
Bull Sequana XH1110	TBD	Affected	
Bull Sequana XH1120 Bull Sequana XH1125	TBD	Affected	
Bull Sequana XH1210		Affected	
Bull Sequana XH1310	N/A	Not affected	Not using a vulnerable CPU.
Bull Sequana XH2135	TS 65.02	Affected	ETA: March 15th
Bull Sequana XH2410 Bull Sequana XH2415	N/A	Not affected	Not using the vulnerable BIOS.

Enterprise	Fixed Version	Status	Comments
Bull Sequana SA	N/A	Not affected	Not using the vulnerable BIOS.
Bullion S	TBD	Affected	
BullSequana M7200 & M7200V (GCOS7)	TS 54.01	Affected	ETA: March 31st
BullSequana M9600 (GCOS8)	TS 54.01	Affected	ETA: March 31st
Bull Sequana S	TS 54.01	Affected	ETA: March 31st

Edge Servers	Fixed Version	Status	Comments
Bull Sequana Edge nano	N/A	Not affected	Not using the vulnerable BIOS.
Bull Sequana Edge	TBD	Affected	

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

Although ATOS makes effort to provide accurate and complete information, ATOS 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

Atos recommends applying Technical States upgrade on its servers as soon as they are made available. As a special recommendation, and due to the nature of the vulnerabilities, it is recommended to apply upgrade on all components of the Technical State to mitigate the risk of a previous successful exploitation. Successful exploitation of these vulnerabilities remains hypothetical at this time.

Available Vendor Patches

Patches are made available as soon as they are validated. Atos is working with its suppliers to distribute updates as soon as possible.

Available Workarounds

No workaround is available.

Available Mitigations

Administrative access on the host is a prerequisite to the exploitation of these vulnerabilities.

Available Exploits/PoC

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

Details

Technical details are available online:

1. https://www.insyde.com/security-pledge
2. https://kb.cert.org/vuls/id/796611.

References

1. https://www.binarly.io/posts/An_In_Depth_Look_at_the_23_High_Impact_Vulnerabilities/index.html.

List of changes

Version	Date	Description
0.1	02/02/2022	First neutralization version
0.2	03/02/2022	Indication of the products which will be fixed. Bullion S added in the list of affected products. Clarification on the dates of the CVEs.
0.3	04/02/2022	Adding products in scope of investigation. Suppression of duplicate CVEs affecting other vendors' products.
0.4	18/02/2022	Reorganizing tables of products. Updated status.
1.0	10/03/2022	First remediation version
2.0	30/05/2022	First public version

Glossary of terms

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. Security bulletins issued during this phase are numbered 0.x.
POC	Proof of Concept
Remediation	The remediation phase ends with the delivering of a qualified solution/update fixing the vulnerability without regression. Security bulletins issued during this phase are numbered 1.x when private. Publicly disclosed bulletins are numbered 2.x.
TI	Threat Intelligence
TLP	Traffic Light Protocol
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

ATOS continuously monitors the security of its products. This Security Bulletin is shared under the constraints of the Traffic Light Protocol (TLP)[1] to bring attention of owners of the potentially affected ATOS products. ATOS recommends that all product owners determine whether the described situation is applicable to their individual case and take appropriate action.

Although ATOS makes effort to provide accurate and complete information, ATOS 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 ATOS 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. The information in this document is subject to change without notice. Product and company names mentioned herein may be trademarks of their respective owners.

About Atos

Atos is a global leader in digital transformation with 107,000 employees and annual revenue of over € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 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), listed on Euronext Paris and included on the CAC 40 ESG and Next 20 Paris Stock Indexes.

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.

[1] https://www.cisa.gov/tlp