EVIDEN
an atos business

Security Bulletin

Misconfiguration of SMC xScale leads to sensitive data exposure

Author(s)	:	Eviden PSIRT
Reference	:	PSIRT-1369
Created	:	24 June 2024
Version	:	2.7
Status	:	Remediation
TLP Classification	:	CLEAR
Document date	:	11 December 2024
Keywords	:	CVE-2024-42018

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

© Copyright 2024, Eviden SAS All rights reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner. For any questions or remarks on this document, please contact Eviden PSIRT gmpl-bds-psirt@eviden.com

List of changes

Version	Date	Description
0.1	2024/06/24	Initial Eviden bulletin
0.2	2024/06/25	Recommendation to assess impact added. Automated and more detailed workaround procedure with check test. More detailed impact analysis.
0.3	2024/06/26	Root cause analysis clarified. Simplified workaround procedure.
1.4	2024/06/27	Available fix. Clarification of check test. TLP:GREEN.
1.5	2024/08/08	CVE id added
2.6	2024/10/09	TLP changed for CLEAR. Minor changes
2.7	2024/12/11	Acknowledgment added to sec. bulletin

Executive summary

A misconfiguration of SMC xScale leads to unexpected exposure of sensitive data upon reboot of diskful nodes.

Vulnerability Info

During initialization of nodes, some configuration parameters are retrieved from management nodes by SMC xScale. These parameters embed credentials whose integrity and confidentiality may be important to the security of the HPC configuration. As these parameters are needed for initialization, there is no available mechanism to ensure access control on the management node, and a mitigation measure is normally put in place to prevent access to unprivileged users.

It was discovered that this mitigation measure does not survive a reboot of the diskful nodes. Diskless nodes are not at risk.

The root cause analysis confirmed that the mistake lies in the cloudinit configuration. The iptables configuration should have been in `bootcmd` instead of `runcmd` section.

CVE No.	CVSS Score	Type of Vulnerability
CVE-2024-42018	7.5	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:H/RL:W/RC:C

The confidentiality of the system parameters of a given node should not rely on a measure applied on every node. The management node should support the corresponding security function.

Affected products

Products	Fixed version	Status	Comments
SMC xScale	1.6.6	Fixed	All previous versions are affected. Released: 2024/06/27

Although Eviden tries 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

If some diskful nodes have been rebooted, we recommend identifying what sensitive data could possibly have been exposed, as it depends on the specific context and adjustments which may have occurred during HPC lifecycle.

Available Vendor Patches

A validated fixed version is available.

Available Workarounds

For workaround or further information, please contact your support.

Available Mitigations

The sensitive URLs are not public.

Available Exploits/PoC

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

Acknowledgment

We wish to thank the team from Juelich Supercomputing Centre at Forschungszentrum Juelich GmbH for initially reporting this finding.

References

1. SMC-xScale-1.6 Administration Guide
2. Slurm 2.14.2 Installation Guide

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 the 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 tries to provide accurate and complete information, Eviden shall not be liable for technical or editorial errors contained in this Bulletin. The information 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, BullSequana, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, IDnomic, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Trustway, Visual BI, Worldgrid, X-Perion.
Eviden is a registered trademark. © Eviden SAS, 2024.