EVIDEN
an atos business

Security Bulletin

Multiple vulnerabilities on Slurm 22.05 and Slurm 23.02

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-674**
Created	:	**14 December 2023**
Version	:	**2.2**
Status	:	**Remediation**
TLP Classification	:	**CLEAR**
Document date	:	**3 May 2024**
Keywords	:	**CVE-2023-49933 CVE-2023-49934 CVE-2023-49935 CVE-2023-49936 CVE-2023-49937 CVE-2023-49938**

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
1.0	2023/12/17	Initial remediation version.
1.1	2024/01/26	Update of CVE scores. Added CVE-2023-49934 precision.
2.2	2024/05/03	TLP:CLEAR version of the bulletin

Executive summary

SchedMD informed about responsible disclosure of a set of security vulnerabilities within Slurm.

The maintenance releases - 23.11.1, 23.02.7, and 22.05.10 include fixes for these issues.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2023-49933	7.5	Improper Enforcement of Message Integrity During Transmission in a Communication Channel AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CVE-2023-49934	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2023-49935	8.8	Insufficient Session Expiration AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2023-49936	7.5	NULL Pointer Dereference AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2023-49937	9.8	Double Free AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2023-49938	8.2	TBD AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

CVE-2023-49933 - Slurm Protocol Message Extension. (Slurm 22.05, 23.02, 23.11.)
Allows for malicious modification of RPC traffic that bypasses the message hash checks.

CVE-2023-49934 - SQL Injection. (Slurm 23.11.)
Arbitrary SQL injection against SlurmDBD's SQL database.

CVE-2023-49935 - Slurmd Message Integrity Bypass. (Slurm 23.02 and 23.11.)
Permits an attacker to reuse root-level authentication tokens when interacting with the slurmd process, bypassing the RPC message hashes which protect against malicious credential reuse.

CVE-2023-49936 - Slurm NULL Pointer Dereference. (Slurm 22.05, 23.02, 23.11.)
Denial of service.

CVE-2023-49937 - Slurm Protocol Double Free. (Slurm 22.05, 23.02, 23.11.) Denial of service, potential for arbitrary code execution.

CVE-2023-49938 - Slurm Arbitrary File Overwrite. (Slurm 22.05 and 23.02.)

Permits an attacker to modify their extended group list used with the sbcast subsystem, and open files with an incorrect set of extended groups.

Affected products

In the table below the indicated version patches the vulnerabilities.

HPC Management Software	RHEL 7.9	RHEL 8.6 EUS	RHEL 8.7 (EOL)	RHEL 8.8	RHEL 9.2
SMC 1.3					
SMC 1.4					
SMC 1.5			2.8.10		
SMC 1.6				2.10.1	2.10.1
SMC xScale 1.1		2.5.9			
SMC xScale 1.2			2.8.10		
SMC xScale 1.5				2.10.1	
SCS5	22.05.10-2			22.05.10-2	
SCS5_LATEST	23.02.6-2			23.02.6-2	

It should also be noted that:

- slurm 2.5.9 includes only 22.05.10-BullSequana.1.1
- slurm 2.8.10 includes 22.05.10-BullSequana.1.1 and 23.02.6-BullSequana.1.1
- slurm 2.10.1 includes 22.05.10-BullSequana.1.1 and 23.02.6-BullSequana.1.1
- CVE-2023-49934 is only affecting version 23.11 (not applicable to the versions provided)

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 the new versions as soon as they are made available.

Available Vendor Patches

Slurm versions 23.11.1, 23.02.7, 22.05.11 are now available and address these security issues.

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://lists.schedmd.com/pipermail/slurm-announce/2023/000103.html

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.