Security Bulletin:

Critical security vulnerabilities in Slurm

Author : Atos BDS TI Team
Created : 2022-05-06
Last Update : 2022-09-14
Revision : 2.1
Keywords :

TLP:WHITE

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

Executive summary

On May 4th, 2022, SchedMD released a security advisory to address 3 critical vulnerabilities patched in Slurm versions 21.08.8 and 20.11.9.

The Slurm Workload Manager, formerly known as Simple Linux Utility for Resource Management (SLURM), or simply Slurm, is a free and open-source job scheduler for Linux and Unix-like kernels, used by many of the world's supercomputers and computer clusters.

It provides three key functions:

- allocating exclusive and/or non-exclusive access to resources (computer nodes) for users for some duration of time so they can perform work,
- providing a framework for starting, executing, and monitoring work, typically a parallel job such as Message Passing Interface (MPI) on a set of allocated nodes, and
- arbitrating contention for resources by managing a queue of pending jobs.

The vulnerabilities are tracked as CVE-2022-29500, CVE-2022-29501 and CVE-2022-29502.

We have not noted any impact to the security of our enterprise services and have not experienced any degraded service availability due to this vulnerability. The main impact of these vulnerabilities is limited to HPC scope.

Vulnerability Info

CVE-2022-29500:

An architectural flaw with how credentials are handled can be exploited to allow an unprivileged user to impersonate the SlurmUser account. Access to the SlurmUser account can be used to execute arbitrary processes as root.

This issue impacts all Slurm releases since at least Slurm 1.0.0.

Systems remain vulnerable until all slurmdbd, slurmctld, and slurmd processes have been restarted in the cluster.

Once all daemons have been upgraded sites are encouraged to add "block_null_hash" to CommunicationParameters. That new option provides additional protection against a potential exploit.

CVE-2022-29501:

An issue was discovered with a network RPC handler in the slurmd daemon used for PMI2 and PMIx support. This vulnerability could allow an unprivileged user to send data to an arbitrary unix socket on the host as the root user.

CVE-2022-29502:

An issue was found with the I/O key validation logic in the srun client command that could permit an attacker to attach to the user's terminal, and intercept process I/O. (Slurm 21.08 only.)

Due to the severity of the CVE-2022-29500 vulnerability, SchedMD removed all prior Slurm releases from official download website.

CVE No.	CVSS Score	Type of Vulnerability
CVE-2022-29500	9.2	AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:X/RL:O/RC:C CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
CVE-2022-29501	8.9	AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:H/E:X/RL:O/RC:C CWE-284: Improper Access Control
CVE-2022-29502	4.9	AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:X/RL:O/RC:C CWE-284: Improper Access Control

Affected products

All products using Slurm are potentially affected, namely SCS5, and SMC/SMCcScale. Please use following repackaged Slurm components.

Atos Product line	Fixed Version	Status	Comments
Slurm 19		Affected	No fix will be provided for this version
Slurm 20	20.11.9	Patched	20.11 remains a temporary solution as 20.11 EOL is expected soon with the coming introduction of 22.05.
Slurm 21	21.08.8	Patched	
Slurm 22	22.05.3	Not affected	First release candidate occurred after fix

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

SchedMD only issues security fixes for the supported releases (which currently are 21.08 and 20.11). Due to the complexity of these fixes, we do not recommend attempting to backport the fixes to older releases, and strongly encourage to upgrade to newest versions.

Customers which still use Slurm in version 19.05, are strongly advised to update the software. At the same time it is important to note that upgrade to 20.11 version remains a temporary solution as 20.11 EOL (End of Life) is expected soon with the release of 22.05 version.

Available Vendor Patches

Slurm versions 21.08.8 and 20.11.9 are available to address the described security vulnerabilities.

Available Workarounds

No workarounds are available.

Available Mitigations

No mitigations are available.

Available Exploits/PoC

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

Details

Technical details are available online:

1. https://github.com/SchedMD/slurm/commit/500787548cf3da22cc69ca2111ce51f77543849b
2. https://github.com/SchedMD/slurm/commit/5b78f713f4b2e390ce80ad754b1240ad36e355ee

References

1. https://www.schedmd.com/news.php
2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29500
3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29501
4. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29502

List of changes

Version	Date	Description
1.0	2022/05/11	First remediation version
2.0	2022/07/15	Public version
2.1	2022/09/14	Updated with Slurm 22.05.3 release

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. 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

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

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.