EVIDEN
an atos business

Security Bulletin

Vulnerability in OpenPMIx

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-486**
Created	:	**27 September 2023**
Version	:	**2.5**
Status	:	**Remediation**
TLP Classification	:	**CLEAR**
Document date	:	**4 March 2024**
Keywords	:	**CVE-2023-41914, CVE-2023-41915**

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	2023/11/07	First remediation version
1.1	2023/11/10	Migration to Eviden template. Indication of RHEL status. Internal fix repositories added.
1.2	2023/12/05	Adding information about vulnerability CVE-2023-41914
1.3	2023/12/18	Adding internal reference.
2.4	2024/02/10	Public issuance
2.5	2024/03/04	Minor changes to fix an upload bug.

Executive summary

OpenPMIx PMIx before 4.2.6 and 5.0.x before 5.0.1 could permit a malicious user to obtain ownership of an arbitrary file on the filesystem when parts of the PMIx library are called by a process running as uid 0. This may happen under the default configuration of certain workload managers, including Slurm. A security issue was reported by François Diakhate (CEA) which is addressed in the PMIx v4.2.6 and v5.0.1 releases. Older PMIx versions are vulnerable but are no longer supported as main stream.

SchedMD Slurm 23.02.x before 23.02.6 and 22.05.x before 22.05.10 allows filesystem race conditions for gaining ownership of a file, overwriting a file, or deleting files.

Eviden SMC and Slurm stacks provide PMIx packages based on OpenPMIx PMIx 3.1.5-2.

PMIx packages have been updated. It is recommended to update the configuration with the indicated version.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2023-41914	7.0	CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2023-41915	8.1	CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Affected products

HPC Management Software	RHEL 7.9	RHEL 8.6 EUS	RHEL 8.7 (EOL)	RHEL 8.8
SMC 1.3		pmix-3.1.5-2 Slurm: 20.11, 21.08, 22.05		
SMC 1.4			pmix-3.1.5-2 Slurm: 21.08, 22.05, 23.02	
SMC 1.5			pmix-3.1.5-2 Slurm: 21.08, 22.05, 23.02	
SMC 1.6				pmix-3.1.5-2 Slurm: 22.05, 23.02
SMC xScale 1.1		pmix-3.1.5-2 Slurm: 22.05		
SMC xScale 1.2			pmix-3.1.5-2 Slurm: 21.08, 22.05	
SMC xScale 1.5				pmix-3.1.5-2 Slurm: 22.05, 23.02
SCS5	pmix-3.1.5-2 Slurm: 21.08, 22.05	pmix-3.1.5-2 Slurm: 20.11, 21.08, 22.05		

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

Note: RHEL 8.4 is no more supported except for custom configuration.

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

It is recommended to upgrade openpmix/openpmix to version 4.2.6, 5.0.1 or higher.

For 3.1.5, pmix-3.1.5-2 contains packages for several Slurm, SMC, SMC xScale and standalone installations.

Eviden recommends applying its Technical States upgrade on its servers as soon as they are made available.

PMIx packages should be updated, customers are strongly encouraged to update their configuration.

Available Vendor Patches

At the moment, the only validated patches are PMIx version 4.2.6, 5.0.1 or higher.

For 3.1.5, Eviden pmix-3.1.5-2 contains packages for several Slurm, SMC , SMC xScale and standalone installations.

We do not provide a link to software as the path is dependent of the channel used by the customer to get the softwares. Some customers may have an account on our external server for software download and path depends on the product orders by the customer (pmix is provided with both Slum and Bull OpenMPI).

We have patched our current version of Slurm with a fix for CVE-2023-41914 vulnerability and we are providing EFIX for both Slurm 22.05 and 23.02.

For some customers, products are downloaded by the local team managing the customer support relationship.

Fix repositories are internally available on the HPC suppport server for all the technical teams:

SMC / SMC xScale

CVE-2023-41915

- https://hpc-support.frbc.bull.fr/dist/ATOS/HPC/pmix/315.1.9/

CVE-2023-41914

- RHEL 8.6 – SMC xScale 1.1:

hpc-support:/dist/ATOS/HPC/slurm/2.5.8_EFIX

- RHEL 8.7 – SMC 1.4 and SMC 1.5:

hpc-support:/dist/ATOS/HPC/slurm/2.8.8_EFIX

- RHEL 8.8 – SMC 1.6:

hpc-support:/dist/ATOS/HPC/slurm/2.9.6_EFIX

SCS5

CVE-2023-41915

- https://hpc-support.frbc.bull.fr/dist/Bull/SCS5/rhel7/x86_64/R3/FIX/Bull_Openmpi/Packages/
- https://hpc-support.frbc.bull.fr/dist/Bull/SCS5/rhel7/x86_64/R3_latest/FIX/Bull_Openmpi/Packages/
- https://hpc-support.frbc.bull.fr/dist/Bull/SCS5/rhel8/x86_64/R3/FIX/Bull_Openmpi/Packages/
- https://hpc-support.frbc.bull.fr/dist/Bull/SCS5/rhel8/x86_64/R3_latest/FIX/Bull_Openmpi/Packages/

CVE-2023-41914:

- hpc-support:/dist/Bull/SCS5/{rhel7,rhel8}/x86_64/R3/EFIX/Bull_Slurm-CVE-2023-41914
- hpc-support:/dist/Bull/SCS5/{rhel7,rhel8}/x86_64/R3_latest/EFIX/Bull_Slurm-CVE-2023-41914

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://nvd.nist.gov/vuln/detail/CVE-2023-41915
2. https://github.com/openpmix/openpmix/releases/tag/v4.2.6
3. https://github.com/openpmix/openpmix/releases/tag/v5.0.1
4. https://docs.openpmix.org/en/latest/security.html
5. https://security.snyk.io/vuln/SNYK-UNMANAGED-OPENPMIXOPENPMIX-5891141
6. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41915

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.*