EVIDEN
an atos business

Security Bulletin

EXAScaler and Lustre User Namespace Security Exploit

Author(s)	**:**	**Eviden PSIRT**
Reference	**:**	**PSIRT-775**
Created	**:**	**19 January 2024**
Version	**:**	**2.2**
Status	**:**	**Remediation**
TLP Classification	**:**	**CLEAR**
Document date	**:**	**19 January 2024**
Keywords	**:**	**CVE-2023-51786**

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 2023, 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@atos.net

List of changes

Version	Date	Description
0.1	2024/01/19	Initial Neutralization version
2.2	2024/01/19	Remediation version. TLP-CLEAR as the information is public. Proposed CVSS.

Executive summary

EXAScaler users can gain access to files or folders in the filesystem that they do not have permission to access based on their user or group ID. This can lead to potential data compromise or privilege escalation. Unauthorized access is limited to subdirectory mountpoints or nodemaps that are visible in the client mountpoint.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2023-51786	8.5	AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

There are two separate issues that, when combined, trigger this vulnerability. Please refer to DDN bulletin for details.

Affected products

This issue affects both EXAScaler and community versions of Lustre.

The following DDN EXAScaler versions are vulnerable:

- EXAScaler 5.x releases from 5.2.0 (2.12.3-ddn43) through 5.2.8 (2.12.9-ddn36)
- EXAScaler 6.x releases from 6.0.0 (2.14.0-ddn13) through 6.2.0 (2.14.0-ddn124)

Recommendations

Eviden recommends applying the security patches as soon as possible.

The security vulnerability is removed by upgrading all clients and MDS servers to the following:

- EXAScaler 5.x patch 2.12.9-ddn37 and higher
- EXAScaler 6.x patch 2.14.0-ddn125 and higher
- Community Lustre 2.15.4 and higher

OSS servers should be upgraded as well to maintain consistent product versions across all servers.

Follow the standard upgrade procedure described in the EXAScaler Installation and Upgrade Guide. As with any other upgrade, this requires upgrading the kmod-lustre RPM for the affected systems along with matching lustre RPMs.

Available Vendor Patches

- EXAScaler 5.x patch 2.12.9-ddn37 and higher
- EXAScaler 6.x patch 2.14.0-ddn125 and higher
- Community Lustre 2.15.4 and higher

Available Workarounds

As a temporary workaround until a patch can be deployed, disable user namespaces on unpatched clients.
DISABLING USER NAMESPACES

To disable user namespaces, run the following command as root on all client nodes:

```
sysctl -w user.max_user_namespaces=0
```

ALERT! This setting completely disables user namespaces on the client. This may cause Docker and other virtualization containers, or other applications employing user namespaces, to run improperly or fail.

RE-ENABLING USER NAMESPACES

After the patch has been applied to a client, re-enable user namespaces. Run the following commands as root on each client node:

```
rm -f /etc/sysctl.d/99-disable-user-ns.conf
sysctl -w user.max_user_namespaces=10000
```

This may be done one client at a time as patches are applied, or on all clients at once after all have been patched.

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-2023-51786
2. https://www.ddn.com/support/resources/security-alerts/
3. https://www.ddn.com/support/resources/important-bulletins/

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

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.