an atos business

Security Bulletin

Vulnerabilities in Keycloak

Author(s)	**:**	**Eviden PSIRT**
Reference	**:**	**PSIRT-1031**
Created	**:**	**26 January 2024**
Version	**:**	**2.5**
Status	**:**	**Remediation**
TLP Classification	**:**	**CLEAR**
Document date	**:**	**6 August 2024**
Keywords	**:**	**CVE-2023-6134, CVE-2023-6563, CVE-2023-6927**

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
0.1	2024/01/26	Initial Neutralization version
0.2	2024/02/02	Added CVE-2023-6134
0.3	2024/05/31	Simplification of tables
1.4	2024/06/28	Remediation version for SMC and SMC xScale updated
2.5	2024/08/06	TLP changed for CLEAR

Executive summary

Keycloak released 23.0.4 version which mitigates the vulnerabilities covered in this bulletin. An attacker can exploit one of these vulnerabilities by creating just two offline tokens. Once these tokens are created, the attacker can interact with the endpoint by triggering a list of the multiple sessions of the user. In environments where there could be potentially millions of offline tokens created by all users, this action leads to an excessive consumption of server memory. In case of vulnerability with a lower score an attacker can steal authorization codes or tokens from clients using a wildcard in the JARM response mode "form_post.jwt".

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2023-6134	5.4	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-74 Improper Neutralization of Special Elements in Output Used by a Downstream Component
CVE-2023-6563	7.1	CWE-770 Allocation of Resources Without Limits or Throttling
CVE-2023-6927	6.1	CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

CVE-2023-6134

A flaw was found in Keycloak that prevents certain schemes in redirects, but permits them if a wildcard is appended to the token. This issue could allow an attacker to submit a specially crafted request leading to cross-site scripting (XSS) or further attacks. This flaw is the result of an incomplete fix for CVE-2020-10748.

CVE-2023-6563

An unconstrained memory consumption vulnerability was discovered in Keycloak. It can be triggered in environments which have millions of offline tokens (> 500,000 users with each having at least 2 saved sessions). If an attacker creates two or more user sessions and then open the "consents" tab of the admin User Interface, the UI attempts to load a huge number of offline client sessions leading to excessive memory and CPU consumption which could potentially crash the entire system.

CVE-2023-6927

A flaw was found in Keycloak. This issue may allow an attacker to steal authorization codes or tokens from clients using a wildcard in the JARM response mode "form_post.jwt" which could be used to bypass the security patch implemented to address CVE-2023-6134.

Affected products

Products	Fixed version	Status	Comments
auth-idp	2.3.3	Fixed	Fixed with Keycloak 23.0.4
SMC	1.8	Fixed	SMC 1.8 includes auth-idp 2.4.5 (with Keycloak 23.0.7)
SMC xScale	1.6	Fixed	SMC xScale 1.6 includes auth-idp 2.4.3 (with Keycloak 23.0.7)

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.

TBD (to be defined) indicates that a new technical state fixing the vulnerabilities is under study.

Unpatched means that the vulnerability is presumably present, but there is no plan to provide a fix. This can be investigated on demand.

Recommendations

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

Available Vendor Patches

See references.

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://www.keycloak.org/2024/01/keycloak-2304-released.html
2. https://nvd.nist.gov/vuln/detail/CVE-2023-6563
3. https://nvd.nist.gov/vuln/detail/CVE-2023-6927
4. https://access.redhat.com/security/cve/CVE-2023-6927
5. https://access.redhat.com/security/cve/CVE-2023-6563
6. https://github.com/keycloak/keycloak/issues/13340
7. https://bugzilla.redhat.com/show_bug.cgi?id=2253308
8. https://bugzilla.redhat.com/show_bug.cgi?id=2255027
9. https://access.redhat.com/errata/RHSA-2024:0094
10. https://access.redhat.com/errata/RHSA-2024:0095
11. https://access.redhat.com/errata/RHSA-2024:0096
12. https://access.redhat.com/errata/RHSA-2024:0097
13. https://access.redhat.com/errata/RHSA-2024:0098
14. https://access.redhat.com/errata/RHSA-2024:0100
15. https://access.redhat.com/errata/RHSA-2024:0101
16. https://access.redhat.com/errata/RHSA-2023:7854
17. https://access.redhat.com/errata/RHSA-2023:7855
18. https://access.redhat.com/errata/RHSA-2023:7856
19. https://access.redhat.com/errata/RHSA-2023:7857
20. https://access.redhat.com/errata/RHSA-2023:7858
21. https://nvd.nist.gov/vuln/detail/CVE-2023-6134
22. https://access.redhat.com/security/cve/CVE-2023-6134

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.