EVIDEN
an atos business

Security Bulletin

Multiple vulnerabilities in Elastic products (Kibana and Elasticsearch)

Author(s)	:	**Eviden PSIRT**
Reference	:	**PSIRT-2079**
Created	:	**16 May 2025**
Version	:	**0.3**
Status	:	**Neutralization**
TLP Classification	:	**CLEAR**
Document date	:	**16 May 2025**
Keywords	:	**CVE-2024-37284 CVE-2024-43709 CVE-2024-52973**

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	2025/02/19	Initial Eviden version
0.2	2025/03/18	Added fix version
0.3	2025/05/16	TLP changed for CLEAR

Executive summary

CVE-2024-37284 - 5.5 (Medium)

Elastic Defend Improper Handling of Alternate Encoding Leads to Crash (ESA-2024-24)

Improper handling of alternate encoding occurs when Elastic Defend on Windows systems attempts to scan a file or process encoded as a multibyte character. This leads to an uncaught exception causing Elastic Defend to crash which in turn will prevent it from quarantining the file and/or killing the process.

CVE-2024-43709 - 6.5 (Medium)

Elasticsearch allocation of resources without limits or throttling leads to crash (ESA-2024-25)

An allocation of resources without limits or throttling in Elasticsearch can lead to an OutOfMemoryError exception resulting in a crash via a specially crafted query using an SQL function.

CVE-2024-52973 - 6.5 (Medium)

Kibana allocation of resources without limits or throttling leads to crash (ESA-2024-26)

An allocation of resources without limits or throttling in Kibana can lead to a crash caused by a specially crafted request to /api/log_entries/summary. This can be carried out by users with read access to the Observability-Logs feature in Kibana.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2024-37284	5.5	Improper Handling of Exceptional Conditions
CVE-2024-43709	6.5	Allocation of Resources Without Limits or Throttling
CVE-2024-52973	6.5	Allocation of Resources Without Limits or Throttling

Eviden is investigating the exact nature of these vulnerabilities to provide validated remediation.

Affected products

Products	Fixed version	Status	Comments
Elastic	8.13.3	Fixed	
Elastic	7.17.21	Fixed	
Kibana	7.17.23	Fixed	
Kibana	8.14.2	Fixed	

Although Eviden tries 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 version 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.

List of HPC Management products

Products	Fixed version	Status	Remaining vulnerabilities
SMC xScale 1.6	1.6.10	Fixed	

Recommendations

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

Available Vendor Patches

No validated patch is available at the time. Eviden is working with its suppliers to distribute updates as soon as possible.

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.cert.ssi.gouv.fr/avis/CERTFR-2025-AVI-0050/
2. https://discuss.elastic.co/t/elastic-defend-8-13-3-security-update-esa-2024-24/373441
3. https://discuss.elastic.co/t/elasticsearch-7-17-21-and-8-13-3-security-update-esa-2024-25/373442
4. https://discuss.elastic.co/t/kibana-7-17-23-and-8-14-2-security-update-esa-2024-26/373443

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 the 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 tries to provide accurate and complete information, Eviden shall not be liable for technical or editorial errors contained in this Bulletin. The information 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, BullSequana, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, IDnomic, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Trustway, Visual BI, Worldgrid, X-Perion.