

## **Security Bulletin**

# **Vulnerability in MongoDB**

Author(s)	:	Eviden PSIRT
Reference	:	PSIRT-1741
Created	:	20 February 2025
Version	:	2.5
Status	:	Remediation
TLP Classification	:	CLEAR
Document date	:	29 March 2025
Keywords	:	CVE-2024-8305 CVE-2024-10921 CVE-2025-0755

#### 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



Vulnerability in MongoDB - CVE-2024-8305 CVE-2024-10921 CVE-2025-Eviden 0755 PSIRT

#### List of changes

Version	Date	Description
0.1	2024/11/11	Initial Eviden version
1.2	2025/01/28	Status changed for remediation
2.3	2025/02/20	TLP changed for CLEAR
2.4	2025/03/27	CVE-2025-0755 added to bulletin
2.5	2025/03/29	Minor change in wording to clarify the independence between OneBSM and MongoDB server version. Fix version recommended for Mongo DB 7.0 branch (16
		instead of 15).

#### Executive summary

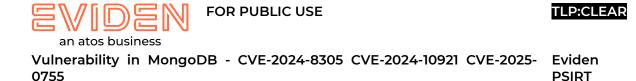
MongoDB informed that unique index may cause secondaries to crash due to incorrect enforcement of index constraints on secondaries, where in extreme cases may cause multiple secondaries crashing leading to no primaries. This issue affects MongoDB Server v6.0 versions prior to 6.0.17, MongoDB Server v7.0 versions prior to 7.0.13 and MongoDB Server v7.3 versions prior to 7.3.4

Second vulnerability: an authorized user may trigger crashes or receive the contents of buffer over-reads of Server memory by issuing specially crafted requests that construct malformed BSON in the MongoDB Server. This issue affects MongoDB Server v5.0 versions prior to 5.0.30, MongoDB Server v6.0 versions prior to 6.0.19, MongoDB Server v7.0 versions prior to 7.0.15 and MongoDB Server v8.0 versions prior to and including 8.0.2.

Third vulnerability (CVE-2025-0755) is in MongoDB C driver. The various bson\_append functions in the MongoDB C driver library may be susceptible to buffer overflow when performing operations that could result in a final BSON document which exceeds the maximum allowable size (INT32\_MAX), resulting in a segmentation fault and possible application crash. This issue affected libbson versions prior to 1.27.5, MongoDB Server v8.0 versions prior to 8.0.1 and MongoDB Server  $\sqrt{7.0}$  versions prior to 7.0.16.

5		
CVE No.	CVSS Score	Type of Vulnerability
CVE-2024-8305	6.5	CWE-1288 Improper Validation of
		Consistency within Input
<u>CVE-2024-10921</u>	6.8	CWE-158 Improper Neutralization of Null
		Byte or NUL Character
CVE-2025-0755	8.4	<u>CWE-122</u> Heap-based Buffer Overflow

#### Vulnerability Info



Eviden is liaising closely with its suppliers and investigating the exact nature of these vulnerabilities to provide validated remediation.

#### Affected products

Products	Fixed version	Status	Comments		
	5.0.30				
	6.0.19	Fixed	Fix for CVE-2024-8305 CVE-2024-10921		
MongoDB	7.0.15	FIXEO	FIX IOF CVE-2024-8305 CVE-2024-1092		
	8.0.3				
MongoDB	8.0.1	Fixed			
Server	7.0.16	Fixed	Fix for CVE-2025-0755		

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 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.

#### List of affected products

Products	Fixed version	Status	Comment					
OneBSM	1.0.1	Fixed	For	already	installed	instances,	it	is
			recommended to update Mongo DB server.					

#### Recommendations

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

#### **Available Vendor Patches**

MongoDB recommends to upgrade versions

- MongoDB Server v5.x versions prior to 5.0.30
- MongoDB Server v6.x versions prior to 6.0.19
- MongoDB Server v7.x versions prior to 7.0.16
- MongoDB Server v8.x versions prior to 8.0.3



Vulnerability in MongoDB - CVE-2024-8305 CVE-2024-10921 CVE-2025- Eviden 0755 PSIRT

Technical States links for Eviden servers are reminded in the table below.

Product	Technical State link
OneBSM	<u>https://support.bull.com/ols/product/platforms/bullion/one-</u> <u>bsm/index.html</u>

### Available Workarounds

For CVE-2025-0755 Eviden recommends to update MongoDB. This can be done without full reinstallation.

## **Available Mitigations**

No mitigation identified.

## Available Exploits/PoC

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

#### References

- 1. <u>https://jira.mongodb.org/browse/SERVER-92382</u>
- 2. https://www.cert.ssi.gouv.fr/avis/CERTFR-2024-AVI-0910/
- 3. https://jira.mongodb.org/browse/SERVER-96419
- 4. https://www.cert.ssi.gouv.fr/avis/CERTFR-2024-AVI-0989/
- 5. https://jira.mongodb.org/browse/SERVER-94461



Vulnerability in MongoDB - CVE-2024-8305 CVE-2024-10921 CVE-2025-Eviden 0755

PSIRT

#### **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.
ТІ	Threat Intelligence
TLP	Traffic Light Protocol (TLP) FIRST Standards Definitions and
	Usage Guidance — Version 2.0. <u>https://www.first.org/tlp/</u>
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.

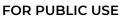
Although Eviden tries to provide accurate and complete information, Eviden shall not be liable for technical or editorial errors contained in this Bulletin. The information is provided "as is" without warranty of any kind. To the extent permitted by the Law, neither Eviden nor its affiliates, subcontractors 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 -



TLP:CLEAR



Vulnerability in MongoDB - CVE-2024-8305 CVE-2024-10921 CVE-2025- Eviden 0755 PSIRT

#### About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of c.  $\in$  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 <u>purpose of Atos</u> 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<sup>1</sup>

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.  $\in$  5 billion.

<sup>&</sup>lt;sup>1</sup> 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. Eviden is a registered trademark. © Eviden SAS, 2025.