

CVE-2025-14847

MongoDB and MongoDB Server Improper Handling of Length Parameter Inconsistency Vulnerability

CISA KEV since Dec 29, 2025

Actively exploited

Public exploit module (Metasploit)

Mismatched length fields in Zlib compressed protocol headers may allow a read of uninitialized heap memory by an unauthenticated client. This issue affects all MongoDB Server v7.0 prior to 7.0.28 versions, MongoDB Server v8.0 versions prior to 8.0.17, MongoDB Server v8.2 versions prior to 8.2.3, MongoDB Server v6.0 versions prior to 6.0.27, MongoDB Server v5.0 versions prior to 5.0.32, MongoDB Server v4.4 versions prior to 4.4.30, MongoDB Server v4.2 versions greater than or equal to 4.2.0, MongoDB Server v4.0

EVRS 84/100 Urgent priority	CVSS V4.0 8.7 High · NVD	EPSS 0.832 99.68th percentile · FIRST	CISA DEADLINE Jan 19, 2026 CISA federal deadline · Overdue by 9 months
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.832 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.7	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability could affect an open-source component, third-party library, protocol, or proprietary implementation that could be used by different products.
Basis: CISA KEV required action

versions greater than or equal to 4.0.0, and MongoDB Server v3.6 versions greater than or equal to 3.6.0.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
mongodb	≥ 3.6.0 < 4.4.30 ≥ 5.0.0 < 5.0.32 ≥ 6.0.0 < 6.0.27 ≥ 7.0.0 < 7.0.28 ≥ 8.0.0 < 8.0.17 ≥ 8.2.0 < 8.2.3	no fixed version listed	NVD

Sources

Vendor guidance	jira.mongodb.org/browse/SERVER-115508	NVD	nvd.nist.gov/vuln/detail/CVE-2025-14847
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-204529
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-14847		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.