Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-14847: Critical MongoDB Memory Leak Exposes Sensitive Data

Date of Publication	Date of Publication	Admiralty Code	TA Number
December 26, 2025	December 29, 2025	A1	TA2025391

Summary

First Seen: December 15, 2025
Affected Products: MongoDB Server
Impact: CVE-2025-14847, dubbed "MongoBleed", is a high-severity, unauthenticated vulnerability in MongoDB Server that allows remote attackers to read sensitive heap memory by exploiting a flaw in Zlib packet decompression. The issue stems from improper validation of compressed data lengths, which causes the server to return uninitialized memory potentially containing credentials, cryptographic keys, or PII to the attacker. This vulnerability affects all major version branches from 3.6 to 8.2, posing a severe risk to any internet-facing database. Active exploitation has been observed in the wild since late December 2025. Shodan data indicates approximately 200,000 MongoDB instances are exposed on the public internet, with 42% of cloud environments containing at least one vulnerable instance. Organizations should immediately upgrade to patched versions (8.2.3, 8.0.17, 7.0.28, 6.0.27, 5.0.32, 4.4.30) or disable zlib compression as a temporary mitigation.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-14847	MongoBleed (MongoDB Server Heap Memory Leak Vulnerability)	MongoDB Server	✗	✓	✓

Vulnerability Details

#1 CVE-2025-14847 is an unauthenticated memory leak vulnerability in MongoDB Server. The vulnerability exists in how MongoDB's server implements zlib compressed protocol headers. Mismatched length fields in the zlib compression handling can cause the server to return uninitialized heap memory in responses to client requests.

#2

An unauthenticated remote attacker can exploit this vulnerability by sending specially crafted requests with manipulated zlib compressed protocol headers to a reachable MongoDB instance. The server processes these malformed requests and responds with memory contents that may include previously handled query data, cached information from other sessions, sensitive configuration data, and potentially credentials or authentication tokens stored in memory.

#3

The exploitation requires no authentication and is of low complexity, making it particularly dangerous for internet-exposed MongoDB deployments. The vulnerability affects MongoDB Server across multiple major versions. These server releases are widely deployed across on-premise and cloud environments and are particularly impactful when internet-facing or reachable from untrusted networks.

#4

Active exploitation of CVE-2025-14847 has been confirmed in the wild. Public proof-of-concept exploits are now available, with exploitation observed shortly after disclosure. Shodan data indicates approximately 200,000 MongoDB instances are exposed on the public internet, with the United States, China, and Germany hosting the highest concentrations. Research data indicates that approximately 42% of cloud environments have at least one MongoDB instance running a vulnerable version. Organizations should immediately upgrade to the patched versions: 8.2.3, 8.0.17, 7.0.28, 6.0.27, 5.0.32, or 4.4.30. If upgrading is not immediately possible, disable Zlib compression in the server configuration to mitigate the risk.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-14847	MongoDB 8.2.0 through 8.2.2 MongoDB 8.0.0 through 8.0.16 MongoDB 7.0.0 through 7.0.27 MongoDB 6.0.0 through 6.0.26 MongoDB 5.0.0 through 5.0.31 MongoDB 4.4.0 through 4.4.29 All MongoDB Server v4.2 versions All MongoDB Server v4.0 versions All MongoDB Server v3.6 versions	cpe:2.3:a:mongodb:mongodb:*:*:*:*:*:*:*:*	CWE-130

Recommendations

Upgrade Immediately to Fixed Versions: The only permanent fix is to upgrade your MongoDB instances to the latest patched releases: 8.2.3+, 8.0.17+, 7.0.28+, 6.0.27+, 5.0.32+, or 4.4.30+. Versions 4.2 and older are End-of-Life (EOL) and will not receive patches, so organizations must plan migration to a supported version to eliminate this risk.

Disable Zlib Compression (Interim Mitigation): If you cannot upgrade immediately, block the attack vector by removing zlib from your server's compression settings. Update your mongod.conf to set net.compression.compressors: snappy,zstd (explicitly excluding zlib) and restart the service to apply the change.

Restrict Network Access to Port 27017: Since this is an unauthenticated remote exploit, ensure your database port is never exposed to the public internet. Use firewalls, VPNs, or Security Groups to allow only trusted application IP addresses, preventing external attackers from establishing the initial connection required for exploitation.

Monitor Logs for Exploit Attempts: Configure your logging or SIEM tools to alert on unexpected connection drops or zlib decompression errors, which can indicate exploitation attempts. While a successful memory leak can be silent, repeated protocol errors or crashes in the mongod process are strong indicators of active scanning or probing.

Rotate Database Credentials Post-Patch: Because the vulnerability leaks uninitialized heap memory, sensitive data like passwords and session tokens residing in RAM may have been exposed. Once you have patched or mitigated the server, rotate all database user credentials and encryption keys to ensure no potentially stolen secrets remain valid.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1595: Active Scanning	T1595.002: Vulnerability Scanning
Resource Development	T1588 : Obtain Capabilities	T1588.006: Vulnerabilities
Initial Access	T1190: Exploit Public-Facing Application	
Collection	T1005: Data from Local System	
	T1213 : Data from Information Repositories	
Credential Access	T1552: Unsecured Credentials	
Discovery	T1082: System Information Discovery	

Patch Details

Upgrade to MongoDB 8.2.3, 8.0.17, 7.0.28, 6.0.27, 5.0.32, or 4.4.30.

Links:
https://www.mongodb.com/try/download/community
https://jira.mongodb.org/browse/SERVER-115508
https://www.mongodb.com/community/forums/t/important-mongodb-patch-available/332977

References

https://jira.mongodb.org/browse/SERVER-115508

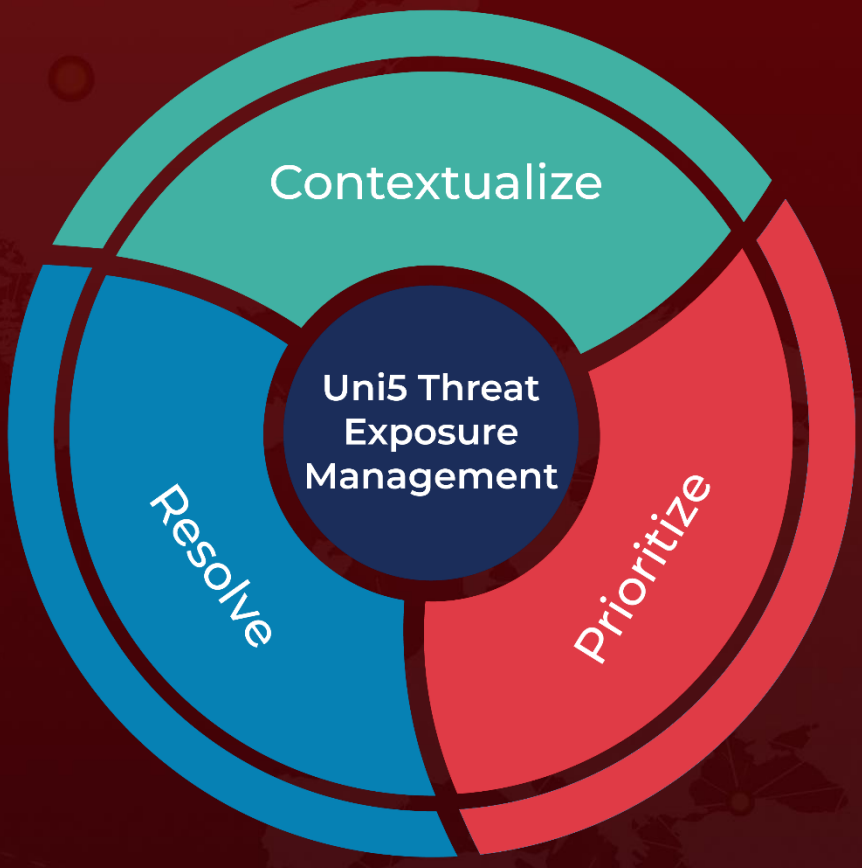
https://www.wiz.io/blog/mongobleed-cve-2025-14847-exploited-in-the-wild-mongodb

https://github.com/joe-desimone/mongobleed

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 26, 2025 • 06:40 AM

More at www.hivepro.com