Executive Summary

1 active priority campaign is currently targeting organizations running exposed MongoDB servers. A critical vulnerability dubbed "**MongoBleed" (CVE-2025-14847)** is being actively exploited in the wild, with a public exploit and full technical details already available. The flaw allows unauthenticated attackers to remotely extract sensitive data directly from server memory — including credentials, API keys, and session tokens — without logging in. An estimated 87,000 servers are currently exposed. A vendor patch is available and should be applied immediately.

Active Threat Campaigns

Campaign	Type	Targets	Key Technique	Priority Action
CVE-2025-14847 MongoBleed (PRIORITY.25.003)	Espionage / Financial	Organizations running exposed MongoDB servers – global	zlib decompression memory miscalculation allows unauthenticated remote memory extraction, leaking credentials, API keys, and session tokens	Patch MongoDB immediately or apply vendor workaround; contact CloudWave Service Desk to identify affected hosted servers

Top 2 Actions This Week

1. Patch MongoDB or Apply the Vendor Workaround Immediately: A patch is available from MongoDB. CloudWave strongly recommends working with your application vendors to upgrade affected MongoDB instances as soon as possible. If an immediate upgrade is not feasible, apply the workaround published by MongoDB: SERVER-115508 Workaround.

2. Rotate Exposed Credentials and Secrets: Because this vulnerability may have already allowed attackers to silently extract data from memory, assume that any credentials, API keys, or session tokens stored or processed by an affected MongoDB server may be compromised. Rotate these secrets proactively as part of your response, even before confirming active exploitation.

CVE-2025-14847 – MongoDB "MongoBleed" Remote Memory Disclosure

MongoDB is a widely deployed database platform used across web applications and services of all sizes. This vulnerability exists in how MongoDB handles zlib compression, a feature used to reduce the size of data transmitted over the network.

Due to a miscalculation in how the code estimates the size of a decompressed message, MongoDB can inadvertently return memory it was not supposed to share. An unauthenticated remote attacker can exploit this to read arbitrary portions of the server's memory — without valid credentials or any prior access. That memory may contain:

- Usernames and passwords
- API keys and tokens
- Active session tokens
- Other sensitive application data

This class of vulnerability is sometimes compared to the "Heartbleed" OpenSSL flaw from 2014, in that it silently leaks sensitive in-memory data without leaving obvious signs of intrusion, making it especially dangerous. A public exploit and full technical write-up are already available, significantly lowering the bar for attackers to take advantage of unpatched systems.

CVSSv3 Score: 8.7 (Critical). The vendor has classified this as a critical fix and released a patch.**Threat Metrics**

Activity Trends	Indicators of Compromise:
• Actively exploited in the wild with public PoC available • Estimated 87,000 MongoDB servers currently exposed globally • Silent exploitation — memory leakage leaves minimal forensic trace • Credential and secret theft may have already occurred on unpatched systems prior to this notification	• Unusual or unexpected inbound connections to MongoDB ports (default: TCP 27017) • Anomalous outbound data transfers from MongoDB servers • Unexpected authentication attempts using recently valid credentials (indicating stolen creds in use) • Evidence of unauthorized API or service access using tokens previously handled by MongoDB

- **Resources:**
- MongoDB Vendor Workaround – SERVER-115508
- NVD – CVE-2025-14847

  MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1552 (Unsecured Credentials), T1005 (Data from Local System)