

MongoDB Vulnerability in Connectivity Suite

Date: 2026-01-21

Version: 1.0

Summary

MongoDB Server is vulnerable to information exposure due to mismatched length fields in Zlib compressed protocol headers. A remote unauthenticated attacker could exploit this issue by sending maliciously crafted requests in order to view uninitialized heap memory.

ID	Title / Description	Severity
CVE-2025-14847	MongoDB Server Vulnerable to Information Exposure via Mismatched Length Fields in Zlib Implementation	CVSS v4.0: 8.7

Affected Products

Brand	Product Line	Affected Version(s)
NetModule	Connectivity Suite	3.7.5 and lower

Mitigation

We recommend to upgrade the MongoDB docker image to the latest patch version. This can be done as follows in a maintenance window:

```
# Change directory to where your compose-file is located
cd ~/cs/app
# Download the latest patch version of the MongoDB docker image
docker compose pull mongodb
# Let docker re-create the MongoDB docker container
docker compose up -d
```

We recommend taking a snapshot of your environment first.

For Help or Feedback

To view all Belden Security Advisories or to report suspected security vulnerabilities, go to <https://www.belden.com/security>.

For technical support and other requests, please visit <https://www.belden.com/support/technical-product-support-main>.

Related Links

- [1] [CVE-2025-14847](#)

Disclaimer

THE SECURITY ADVISORY, AND INFORMATION CONTAINED HEREIN, ARE PROVIDED ON AN "AS IS" BASIS AND DO NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE ADVISORY, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THE ADVISORY, IS AT YOUR OWN RISK. INFORMATION IN THIS ADVISORY AND ANY RELATED COMMUNICATIONS IS BASED ON OUR KNOWLEDGE AT THE TIME OF PUBLICATION AND IS SUBJECT TO CHANGE WITHOUT NOTICE. BELDEN RESERVES THE RIGHT TO CHANGE OR UPDATE ADVISORIES AT ANY TIME.

Revisions

V1.0 (2026-01-21) Security Advisory published.