Vulnerability Disclosure

CA-VD-2026-001

MongoDB component memory disclosure vulnerability (CVE-2025-14847)

Security has always been a focus at ComAp, so our customers can rest assured ComAp always has and always will take the security of customers data and equipment seriously.

ComAp is committed to fix all reported security vulnerabilities quickly and carefully to protect the security and privacy of our users.

Affected products

› InteliSCADA – all versions prior to 3.0 (the bundled MongoDB component contains the vulnerable library).

InteliSCADA is a Microsoft Windows-only application. Supported operating systems are Microsoft Windows 10/11 64-bit and Windows 10/11 IoT 64-bit. The InteliSCADA server runs as the Windows service ComApInteliSCADAService.

Vulnerability ID

ComAp ID: CA-VD-2026-001

CVE ID: CVE-2025-14847 (also tracked publicly as “MongoBleed”)

CWE: CWE-908 – Use of Uninitialized Resource / CWE-130 – Improper Handling of Length Parameter Inconsistency

Summary

A vulnerability (CVE-2025-14847) has been disclosed in the MongoDB Server component which is embedded in InteliSCADA versions prior to 3.0. The flaw is located in MongoDB's zlib message decompression routine and allows an unauthenticated remote attacker to read uninitialized heap memory by sending specially crafted compressed protocol messages. Disclosed memory contents may include fragments of credentials, session tokens, configuration data or other information present in the MongoDB process at the time of the request. The vulnerability has been observed under active exploitation in the wild.

Starting with InteliSCADA 3.0 the embedded MongoDB database has been replaced with PostgreSQL (with the TimescaleDB extension). The vulnerable component is therefore no longer part of the product, and InteliSCADA 3.0 and later releases are not affected by CVE-2025-14847.

Vulnerability Severity

The severity assessment has been performed using the FIRST Common Vulnerability Scoring System (CVSS) v3.1. Two scores are provided: the score published on the official CVE record (upstream, generic MongoDB context) and a ComAp contextual score that reflects how the MongoDB component is actually deployed inside InteliSCADA.

Upstream score (NVD / MongoDB Inc.)

CVSS v3.1 Base Score: 7.5 (High)

CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Reference: https://nvd.nist.gov/vuln/detail/CVE-2025-14847

ComAp contextual score (InteliSCADA deployment)

In a typical InteliSCADA deployment the embedded MongoDB instance is reachable only from the InteliSCADA application server on a local / segmented OT network, not from the public Internet. The Attack Vector is therefore re-scored from Network (N) to Adjacent (A); other metrics remain unchanged.

CVSS v3.1 Base Score: 6.5 (Medium)

CVSS v3.1 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Calculator: https://www.first.org/cvss/calculator/3.1

Remediation

ComAp has addressed the vulnerability by replacing the embedded database in InteliSCADA. Customers running any InteliSCADA release prior to 3.0 are strongly advised to take one of the following actions:

Recommended solution – Upgrade to InteliSCADA 3.0 or later

Update the existing installation to InteliSCADA 3.0 (or any later release). InteliSCADA 3.0 replaces the previously embedded MongoDB database with PostgreSQL (with the TimescaleDB extension); the vulnerable MongoDB component is therefore removed entirely and CVE-2025-14847 no longer applies to the system.

Download the latest InteliSCADA release from the official product page: https://www.comap-control.com/products/software-tools/monitoring-tools/pc-monitoring-tools/inteliscada/

Two paths are supported:

› Upgrade (recommended): performed in-place on top of the existing pre-3.0 installation on the same Windows host. Historical/runtime data (trends, alarm history, event logs, archived values, project configuration) is retained and remains available after the upgrade. The InteliSCADA installer detects an existing installation and offers a built-in backup step ("Backup all data" or "Backup data without trends") – it is recommended to create this backup before proceeding.

› Clean reinstallation: used when an in-place upgrade is not possible or not desired. A clean reinstallation will clear all historical/runtime data from the previous installation. Before starting, create a backup using the InteliSCADA installer's backup step or the DatabaseMaintenanceTool.exe utility (located in …\PC Suite\InteliSCADA\Tools\DatabaseMaintenanceTool\), and store the backup file on an external drive.

Important: Choose the upgrade path if historical data must be preserved. Reinstallation is faster and produces a clean system, but at the cost of losing all stored history. Follow the standard InteliSCADA installation/upgrade guide (see InteliSCADA Global Guide, chapter "Installation" / "Database backup") and contact your local ComAp representative if assistance with the procedure is required.

Alternative solution 1 – Restrict network access to the MongoDB port

If upgrading to InteliSCADA 3.0+ is not immediately possible, the vulnerability can be effectively mitigated by ensuring that the embedded MongoDB service is not reachable from any untrusted network. CVE-2025-14847 is exploited over the MongoDB wire protocol on TCP port 27017 (default); if the attacker cannot reach this port, the vulnerability cannot be triggered remotely.

Recommended steps:

› Verify which TCP port the embedded MongoDB instance is listening on (default: 27017) and on which network interface it is bound.

› Bind MongoDB to localhost (127.0.0.1) or to a dedicated internal management interface only, by setting the bindIp option in mongod.cfg (e.g. bindIp: 127.0.0.1). The InteliSCADA application server is the only client that needs access.

› On the Windows host firewall (Windows Defender Firewall with Advanced Security) explicitly block inbound traffic to the MongoDB port from all external sources, while still allowing local access for the ComApInteliSCADAService.

› On the network/perimeter firewall, ensure the MongoDB port is not forwarded, NAT-ed or otherwise exposed to the Internet or to general office IT networks. The InteliSCADA server should be placed in a segmented OT/SCADA zone.

› After applying the change, verify from an external host that the MongoDB port is no longer reachable (for example using a port scan from outside the trusted segment).

This mitigation is consistent with the intended InteliSCADA deployment architecture and is recommended as a permanent hardening measure, in addition to (not instead of) future upgrades.

Alternative solution 2 – Disable zlib network compression in MongoDB

Where it is not possible to fully restrict network access to the MongoDB port (for example when MongoDB must be reachable across a wider trusted network), the vulnerability can also be mitigated by disabling zlib network message compression on the embedded MongoDB instance. CVE-2025-14847 is located in the zlib decompression path; disabling that compressor removes the attack surface without changing any other MongoDB functionality.

Edit the MongoDB configuration file (typically mongod.cfg) and set the network compressors so that zlib is excluded, for example:

```
net:
  compression:
    compressors: snappy,zstd
```

After saving the configuration, restart the MongoDB service so the change takes effect. Verify the active compressors via the MongoDB log (line containing “compressors”) or by running db.serverStatus().network on an authenticated session.

This workaround is intended as a temporary mitigation only. Customers are still strongly encouraged to upgrade to InteliSCADA 3.0+ at the earliest opportunity.

Vulnerability details

MongoDB Server contains an improper handling of length parameter inconsistency in zlib compressed protocol headers. When a specially crafted OP_COMPRESSED message is received, the server may return content from uninitialized heap memory in the response, which is then sent back to the unauthenticated client. Because zlib compression is enabled by default in MongoDB, all default installations – including the MongoDB instance embedded in InteliSCADA before version 3.0 – are exposed unless network access to the MongoDB port is fully restricted.

Disclosed memory may contain any data the MongoDB process has previously handled, including authentication material, query content, configuration values and other potentially sensitive information. The vulnerability is exploitable remotely, without authentication and without user interaction, and has been added by CISA to the Known Exploited Vulnerabilities (KEV) catalog.

Mitigating Factors

Pay attention to the following recommendations and measures to increase the level of security of ComAp products and services.

Please note that possible cyber-attacks cannot be fully avoided by the below mentioned recommendations and set of measures already performed by ComAp, but by following them the cyber-attacks can be considerably reduced and thereby to reduce the risk of damage. ComAp does not take any responsibility for the actions of persons responsible for cyber-attacks, nor for any damage caused by the cyber-attack. However, ComAp is prepared to provide technical support to resolve problems arising from such actions, including but not limited to restoring settings prior to the cyber-attacks, backing up data, recommending other preventive measures against any further attacks.

Warning: Some forms of technical support may be provided against payment. There is no legal or factual entitlement for technical services provided in connection to resolving problems arising from cyber-attack or other unauthorized accesses to ComAp's Products or Services.

› Do not expose the MongoDB TCP port (default 27017) of the InteliSCADA server to the public Internet. The MongoDB instance is intended to be reachable only from the InteliSCADA application server on a trusted, segmented network.

› Restrict access to the InteliSCADA Windows server using host-level (Windows Defender Firewall) and network-level firewalls, and place it in a dedicated OT/SCADA network segment separated from office IT and Internet-facing zones.

› Enable MongoDB authentication and use strong, unique credentials. Even though CVE-2025-14847 is pre-authentication, authentication and access control reduce the impact of other potential issues.

› Keep InteliSCADA and the underlying Microsoft Windows operating system fully patched (Windows Update, drivers), and monitor MongoDB logs for unusual OP_COMPRESSED traffic, repeated malformed messages or unexpected client connections.

› Where any of the alternative workarounds is applied, plan an upgrade to InteliSCADA 3.0+ to remove the underlying vulnerability permanently.

Support

For further support, please contact your local ComAp representative. For contact information, see https://www.comap-control.com/contact-us/comap-worldwide.

Latest InteliSCADA release: https://www.comap-control.com/products/software-tools/monitoring-tools/pc-monitoring-tools/inteliscada/

ComAp Disclaimer