

Mesalvo Security Advisory

MSA-2026-004: Administrative SQL query tool in MEONA and SQL Server hardening (CVE-2026-22315)

Publisher: Mesalvo Freiburg GmbH, Heinrich-von-Stephan-Str. 25, 79100 Freiburg, Germany · Security contact: isb@mesalvo.com · Distribution: TLP:CLEAR (may be shared without restriction) · Canonical URL: <https://mesalvo.com/en/vdp/advisories/msa-2026-004.pdf>

Advisory ID	MSA-2026-004
CVE	CVE-2026-22315 (CNA: ENISA). Mesalvo disputes the classification of this record as a vulnerability and has requested its rejection as intended functionality and as a duplicate of CVE-2026-0857 (see "Note on the CVE record").
Published / last updated	21 September 2026 / 21 September 2026 – Version 1.1
Severity	Mesalvo assessment CVSS v3.1 Base 6.8 (Medium), Temporal 6.2 (Medium). The CNA record shows 7.2 (High) pending correction.
Status	Intended administrative functionality; no change to the tool planned. The exposure of readable passwords through the tool is removed with MEONA 2025.04.24 and 2026.03.02 (CVE-2026-0857). Operator guidance below.
Patient safety	No impact on patient safety identified. Not a reportable incident under MDR Art. 87.
Misuse	Mesalvo is not aware of any misuse outside the reported security test.

Summary

MEONA provides administrators with a documented SQL query tool ("Spezielle Reports") for preparing report data directly from the MEONA database. The tool is restricted to holders of the super-administrator-level permission `REPORT_GLOBAL`, which the operating hospital assigns. A security test reported the tool as a vulnerability because, in the tested installation, the exported user table contained passwords stored with legacy methods (CVE-2026-0857), and because the SQL Server instance allowed NTLM relay through extended stored procedures. Mesalvo considers the tool intended administrative functionality, treats the readable passwords under CVE-2026-0857, and addresses the SQL Server configuration through the hardening guidance below.

Products and versions concerned

MEONA Server and MEONA Client, all versions, contain the SQL query tool as intended functionality. Readable passwords in the exported data occur only for locally managed accounts stored under a legacy method (accounts authenticated through the hospital's directory service have no password in the MEONA database), and not from MEONA 2025.04.24 and 2026.03.02 onwards (see MSA-2026-002).

Description of the function

Under "Spezielle Reports" → "SQL-Abfragen" in the administration area, a holder of the permission `REPORT_GLOBAL` can save SQL statements that are executed against the MEONA database under the application's database login and use the result as a data source for user-defined reports (MEONA Konfigurationsanleitung 2025.04, Version 1.0, appendix "Reporting", section 2.3.2 "Eigenes Datenmodell mit

SQL-Abfragen erstellen", p. 659; earlier handbook section 48.1.1.2; SQL Querying training). Creation and modification of saved queries are recorded in the MEONA audit tables with user name, host and timestamp.

Mesalvo's position

The tool is intended, documented and restricted to a dedicated administrative permission. An administrator running a query against the database of the system they administer, comparable to a database administrator, does not exploit a vulnerability. What the security test found in the exported data, readable passwords of locally managed accounts, is the weakness described in CVE-2026-0857 and is addressed by its service packs; after their installation the same export contains Argon2 hashes and nothing else, and directory-authenticated users never have a password in the MEONA database. The NTLM relay described by the testers is a property of the Microsoft SQL Server configuration (extended stored procedures such as xp_dirtree, and the service account under which SQL Server runs) and not of MEONA; MEONA does not use or require these procedures. The possibility of reaching the tool without the permission, as in the reported test, is the subject of CVE-2026-0856 and MSA-2026-001.

CVSS

Base (Mesalvo)	CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H – 6.8 (Medium). Privileges Required: High (REPORT_GLOBAL; as in the CNA record). Attack Vector: Adjacent (closed hospital network zone). The CNA record shows AV:N (7.2); Mesalvo has requested correction.
Temporal (Mesalvo)	CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C – 6.2 (Medium). E:P: demonstrated in a security test. RL:T: vendor guidance available; credential exposure addressed by the CVE-2026-0857 service packs. RC:C: confirmed.
Environmental	Installations without accounts on a legacy storage method, or with MEONA 2025.04.24 / 2026.03.02, have no readable passwords in the exported data. Operators should compute their own Environmental score.

Recommendations for operators

- Assign the permission REPORT_GLOBAL only to a small, named group of administrators, under the same approval and review process as database administrator rights; review the assignments now and regularly.
- Review the MEONA audit tables (sql_query_aud) for changes to saved queries and reconcile them with approved reporting tasks.
- Update to MEONA 2025.04.24 or 2026.03.02 within the regular update cycle when available, or apply the recommended operating configuration of MSA-2026-002 now, so that no readable passwords exist in the user table.
- Harden the Microsoft SQL Server instance: run the MEONA database login as a dedicated low-privilege account without sysadmin or serveradmin rights; keep xp_cmdshell and OLE Automation Procedures disabled (sp_configure) and revoke execute rights on extended procedures not required by MEONA (xp_dirtree, xp_fileexist); enforce SMB signing and Extended Protection for the SQL Server instance per Microsoft baseline; restrict the TDS endpoint to the application server hosts.
- Implement the measures of MSA-2026-001 to close the unauthorised access path to the administrative functions.

Assessment under medical device regulation

MEONA is medical device software placed on the market under Article 120 MDR. Mesalvo operates a secure product lifecycle in line with IEC 81001-5-1, of which the handling of externally reported findings, this advisory and the delivery of security hardening in regular maintenance releases are ordinary parts. Mesalvo has assessed the findings described in this advisory within its risk management (ISO 14971) and post-market surveillance processes. The findings concern information-security properties of administrative functions that are reachable only from within the operator's protected hospital network by holders of a valid account, i.e. the part of the shared responsibility for information security that MDCG 2019-16 and IEC 80001-1 assign to the operating healthcare institution (network segmentation, workstation hardening, assignment of administrative permissions). No effect on the clinical performance of MEONA and no risk to patients has been identified. Mesalvo has concluded within its vigilance process that the findings do not constitute an incident within the meaning of Article 87 MDR and do not require a field safety corrective action. The function described is intended administrative functionality of MEONA. No product change is made; the recommendations in this advisory concern the operator's assignment of administrative permissions and the configuration of the database server. This document is a security advisory published under Mesalvo's Vulnerability Disclosure Policy; it is not a Field Safety Notice.

Note on the CVE record

The CVE record as published by the CNA on 20 May 2026 classifies the tool as an "incorrect privilege assignment" enabling the export of cleartext passwords over the network (CVSS 7.2). Mesalvo has requested under the CVE Program dispute policy that the record be rejected as intended administrative functionality and as a duplicate of CVE-2026-0857 or, alternatively, corrected as to description, classification, affected versions and CVSS vector. Mesalvo will update this advisory when the CNA has decided.

Coordination and disclosure

The findings originate from a security test that a customer commissioned from an external security service provider in late 2025. The findings were explained to Mesalvo on 27 January 2026 and provided in writing on 9 February 2026. Mesalvo assessed them and discussed them with the customer and the service provider on 15 April and 4 May 2026. Mesalvo's own analysis did not agree with the finding: the SQL query tool is a documented administrative function restricted to an explicitly assigned administrative permission, its use by a permission holder is not a weakness of the product, and the readable passwords found in the exported data are the subject of CVE-2026-0857. Mesalvo did not agree to a CVE record for this finding. The record was published by the CNA on 20 May 2026 in a form Mesalvo had not reviewed; Mesalvo has requested its rejection, alternatively its correction, under the CVE Program dispute policy (see "Note on the CVE record"). This advisory follows Mesalvo's review of the published record against the product facts. Mesalvo asks security researchers to report vulnerabilities in Mesalvo products to isb@mesalvo.com in accordance with the Mesalvo Vulnerability Disclosure Policy (<https://mesalvo.com/en/vdp>).

References

- CVE record: <https://www.cve.org/CVERecord?id=CVE-2026-22315>
- NVD: <https://nvd.nist.gov/vuln/detail/CVE-2026-22315>
- MSA-2026-001 (CVE-2026-0856), MSA-2026-002 (CVE-2026-0857), MSA-2026-003 (CVE-2026-22314)
- MEONA Konfigurationsanleitung 2025.04, Version 1.0 (21 September 2026; UDI-DI 4262357191084): appendix "Reporting", 2.3.2 "Eigenes Datenmodell mit SQL-Abfragen erstellen" (p. 659) and 2.3.2.1 "SQL-Abfrage verknüpfen" (p. 660); security notice on separation of administrative and end-user duties (p. 39); earlier MEONA administration handbook, section 48.1.1.2
- Mesalvo Vulnerability Disclosure Policy: <https://mesalvo.com/en/vdp>

Revision history

Version	Date	Change
1.0	21 September 2026	Initial publication.
1.1	21 September 2026	Documentation references updated to the MEONA Konfigurationsanleitung 2025.04, Version 1.0, which consolidates the reporting and SQL query documentation as an appendix. No change to the assessment.