Mesalvo Security Advisory

MSA-2026-001: Role check of the MEONA Client and access to the administration area (CVE-2026-0856)

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-2026-001.pdf

Advisory ID	MSA-2026-001
CVE	CVE-2026-0856 (CNA: ENISA)
Published / last updated	21 September 2026 / 21 September 2026 – Version 1.0
Severity	CVSS v3.1 Base 7.8 (High) as published by the CNA. Temporal 7.1 (High). Environmental 6.4 (Medium) for operators enforcing application control on MEONA workstations; 7.1 (High) without. See section "CVSS".
Status	Security hardening included in the regular service packs MEONA 2025.04.24 and 2026.03.02 (Q4 2026). Operator configuration recommendations available now.
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

For access to the administrative functions of the MEONA Client, the MEONA Server relies on the role information supplied by the MEONA Client. A person who holds a valid MEONA user account, has access to the hospital's internal network and is able to execute a modified copy of the MEONA Client can assert an administrator role and access the administrative functions of the MEONA Client (admin panel) with regular user credentials. MEONA is operated exclusively within closed hospital networks and is not exposed to the public Internet.

Products and versions concerned

Product	Versions	Status
MEONA Client	2024.10, all service packs	Behaviour present. End of support; no further service pack. Operator configuration recommendations apply.
MEONA Client	2025.04, service packs before 2025.04.24	Behaviour present. Hardening included in 2025.04.24 (Q4 2026).
MEONA Client	2026.03, service packs before 2026.03.02	Behaviour present. Hardening included in 2026.03.02 (Q4 2026).
MEONA Server	2024.10, 2025.04, 2026.03	Behaviour present. The server accepts the role asserted by the client; see Description.

Description

The MEONA Client transmits the role of the logged-in user to the MEONA Server. The server uses this role to decide whether administrative functions may be used, without independently verifying it against the user's role stored on the server. A user who modifies the MEONA Client so that it transmits the super-administrator role can therefore use the admin panel with a regular user account.

The reported attack modified assemblies of the installed MEONA Client. Mesalvo classifies the weakness as CWE-284 (Improper Access Control).

Conditions under which the behaviour can be misused

1. A valid MEONA user account issued by the operating hospital.
2. Access to the hospital's internal network from a device on which the MEONA Client is installed. MEONA is not reachable from the public Internet; where a hospital permits remote access to that network at all, it is only through the hospital's own remote-access infrastructure (e.g. VPN) under the hospital's control.
3. The ability to modify the MEONA Client binaries and to execute the modified copy on that device. In the security test that led to this record this was possible because the MEONA Client installation folder on the test workstation was writable for the logged-on user. On managed devices with a protected installation folder and application control, as recommended below, this requires local administrator privileges on the device.

Effect on information security

A person who meets all conditions obtains the administrative functions of the MEONA Client: user administration including the display of stored credential data of locally managed accounts (see MSA-2026-002 / CVE-2026-0857), profile and content configuration, form scripting and Spring XML configuration (see MSA-2026-003 / CVE-2026-22314) and the SQL query tool (see MSA-2026-004 / CVE-2026-22315). The administrative functions themselves are documented, intended functions restricted to holders of the corresponding permissions; the weakness described here is the possibility of reaching them without holding those permissions.

CVSS

Base (CNA)	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H – 7.8 (High). Mesalvo does not contest the Base vector. The Base score by design excludes the deployment context and the prerequisites above.
Temporal (Mesalvo)	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C – 7.1 (High). E:P: a proof of concept was demonstrated in a security test; no exploit code is public. RL:T: vendor measures are available (operator configuration guidance now; code signing with integrity verification in 2025.04.24 and 2026.03.02) that do not change the client's role query itself. RC:C: confirmed by Mesalvo.
Environmental – operator following the hardening guidance	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C/CR:H/IR:H/AR:H/MAV:L/MAC:H/MPR:L – 6.4 (Medium). Security requirements CR:H, IR:H, AR:H reflect a clinical information system. MAC:H applies where application control (WDAC/AppLocker) is enforced on MEONA workstations, because the person must additionally defeat that control before a modified client can run. MAV:L and MPR:L are stated explicitly and unchanged: the network position and the regular MEONA account are the same in every

	deployment.
Environmental – operator without application control	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C/CR:H/IR:H/AR:H/MAV:L/MPR:L – 7.1 (High). Identical to the Temporal score: without application control there is no environmental condition that reduces the score. This is the reason the first operator recommendation below is application control.
Your own score	Operators should compute their own Environmental score with the FIRST CVSS v3.1 calculator (https://www.first.org/cvss/calculator/3.1) using the Base and Temporal vectors above and their own Modified metrics and Security Requirements.

Product changes in the regular service packs

MEONA 2025.04.24 and 2026.03.02 (planned for Q4 2026) introduce code signing of all MEONA Client executables and assemblies and integrity verification of the client assemblies at start-up. A modified assembly is detected and the client refuses to start. Together with application control on the workstation, this prevents the reported path. The change is security hardening delivered in the regular service packs; it does not alter the clinical functions or the intended purpose of MEONA.

Mesalvo has assessed the findings within its risk management and post-market surveillance processes (see "Assessment under medical device regulation") and will announce the availability of the service packs through the usual release channels and by updating this advisory.

Recommendations for operators

- Enforce application control (e.g. Windows Defender Application Control or AppLocker) on all MEONA workstations, allowing only signed Mesalvo binaries from the protected installation directory to execute. This blocks the execution of modified client copies from user-writable locations.
- Ensure that the MEONA Client installation folder is not writable for standard users (default NTFS permissions for Program Files). In the security test that led to this record, the modified client could be placed because the installation folder was writable.
- Do not grant local administrator rights on MEONA workstations to clinical users.
- Provision and de-provision MEONA user accounts through the hospital's central identity and access management (Active Directory / Entra ID integration) and review administrative role assignments regularly.
- Keep the MEONA network zone segmented; do not expose the MEONA Server to the Internet or to untrusted network segments; where remote access to the zone exists (e.g. VPN), restrict it to authorised personnel.
- Update to MEONA 2025.04.24 or 2026.03.02 within the regular update cycle when available.

Log review

The MEONA Server logs administrative actions together with the user name of the executing account. Operators can review these logs and compare the logged user names against the permission sets assigned to those users in the MEONA user administration; administrative actions logged for a user without administrative permissions indicate use of this weakness.

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 product changes described above are security hardening delivered in the regular service packs as part of Mesalvo's continuous improvement of information security; they do not change the intended purpose, the clinical functions or the performance of MEONA (non-significant change in the sense of MDCG 2020-3). 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

Mesalvo does not dispute the existence of the weakness described in this advisory. Mesalvo has requested under the CVE Program dispute policy that the record be corrected: a description that states the mechanism (the server relies on the role information supplied by the client) and the conditions for its misuse, the correct product designations (MEONA Client, MEONA Server) and Mesalvo release designations (2024.10, 2025.04, 2026.03, with 2025.04.24 and 2026.03.02 as the service packs containing the hardening), remediation information, this advisory as vendor reference, and the coordination timeline. Mesalvo will update this advisory when the record is changed.

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 findings as presented, in particular regarding the conditions for misuse, the privileges required and the resulting severity; Mesalvo did agree that the behaviour of the role check should be documented in a CVE record that states those conditions. In the discussion of 4 May 2026 Mesalvo therefore agreed to CVE records for CVE-2026-0856 and CVE-2026-0857 subject to its approval of the text. The records were published by the CNA on 20 May 2026 in a form Mesalvo had not reviewed; Mesalvo has requested corrections under the CVE Program dispute policy (see "Note on the CVE record"). This advisory follows Mesalvo's review of the published records against the product facts and the scheduling of the related product changes in the regular service packs.

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-2026-0856
- European Vulnerability Database: https://euvd.enisa.europa.eu/ (search: CVE-2026-0856)
- NVD: https://nvd.nist.gov/vuln/detail/CVE-2026-0856
- Mesalvo Vulnerability Disclosure Policy: https://mesalvo.com/en/vdp

Revision history

Version	Date	Change
1.0	21 September 2026	Initial publication.