Mesalvo Security Advisory

MSA-2026-003: Scripting and Spring XML configuration functions in MEONA administration (CVE-2026-22314)

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-2026-003.pdf

Advisory ID	MSA-2026-003
CVE	CVE-2026-22314 (CNA: ENISA). Mesalvo disputes the classification of this record as a vulnerability and has requested its rejection or correction (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 7.9 (High), Temporal 7.2 (High). The CNA record shows 9.0 (Critical) pending correction; the difference lies in the privileges required (administrative permissions) and the network position (closed hospital network).
Status	Intended administrative functionality; no change to the functions planned. Operator guidance below. The unauthorised access path used in the reported test is addressed in MSA-2026-001.
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 offers administrators documented functions for customer-specific customisation: form scripting, report scripting and Spring.NET XML content configuration. Scripts and configurations defined with these functions are executed by the MEONA Client on the workstations of the users who open the affected forms, reports or profiles. The functions are restricted to holders of dedicated administrative permissions that the operating hospital assigns. A security test reported them as a code-injection vulnerability after reaching them with a regular account through CVE-2026-0856. Mesalvo considers the functions intended administrative functionality and has requested correction of the CVE record. This advisory explains what the functions do, who can use them and how operators should govern them.

Products and versions concerned

MEONA Server and MEONA Client, all versions. The functions are part of the product and remain available.

Description of the functions

Function	Permission	Documentation (Konfigurationsanleitung 2025.04 v1.0; earlier handbook)
Form scripting (Boo) for user-defined forms	USER_DEFINED_FORMS_ADMINISTRATOR	"Benutzerdefinierte Formulare – Skripte" (pp. 253–254); appendix "Skripte" (pp.

Function	Permission	Documentation (Konfigurationsanleitung 2025.04 v1.0; earlier handbook)
		554–648); earlier handbook 11.9, 45.2.6
Report designer script setting (C#, Visual Basic, J#) in user-defined reporting	ADMINISTRATOR or SUPERADMINISTRATOR role plus USER_DEFINED_FORMS_ADMINISTRATOR (the report designer is opened from the administration area, Benutzerdefiniertes Reporting: Ansichten; the script language is a property of the report layout and has no separate permission)	"Benutzerdefiniertes Reporting" (p. 259 ff.); appendix "Reporting" 2.4.4.11 "Skriptsprache einstellen" (p. 667); earlier handbook 48.1.2.12, 48.1.4
Spring.NET XML content configuration (patient window, clinics window)	SPRING_ADMINISTRATOR and XML_CONTENT_EDITOR	Appendix "Spring XML", chapter 6 "Konfiguration im Meona Admin-Bereich" (pp. 743–769); profile options PATIENT_CONTENT_CONFIGURATION, CLINICS_CONTENT_CONFIGURATION
Spring.NET XML object definitions and application editor registry	An administrative role with access to the administration area (ADMINISTRATOR, SUPERADMINISTRATOR, or the restricted administrative role TYPIST (catalogue editing) and the PHARMACIST role holding the PHARMACY_ADMINISTRATOR right)	Appendix "Spring XML", chapter 6 (pp. 743–769)

Scripts are compiled and executed by the MEONA Client on the workstation of the user who opens the form or report, with the privileges of that user's Windows account. Spring.NET XML configurations are loaded by the MEONA Client for every user whose profile references them. The scripts run with the privileges of the logged-in Windows user and are not subject to MEONA permission checks or runtime restrictions at execution; only their creation, editing and compilation are gated. A holder of the permissions above can therefore define code that runs on the workstations of other MEONA users. Every change to scripts and configurations is recorded in the MEONA Server audit log with the executing user.

Mesalvo's position

The functions are intended, documented and restricted to dedicated administrative permissions. Holders of these permissions are administrators appointed by the operating hospital; their ability to define code that runs in MEONA on the hospital's workstations is the purpose of the functions, comparable to a domain administrator deploying scripts to workstations through Group Policy or a device-management platform. Mesalvo therefore does not classify this as a vulnerability of MEONA. The security-relevant question is who holds the permissions and how their use is controlled, which is addressed below. The possibility of reaching these functions without holding the permissions, as in the reported test, is a separate issue (CVE-2026-0856) and is addressed in MSA-2026-001.

CVSS

Base (Mesalvo)	CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H – 7.9 (High). Privileges Required: High (dedicated administrative permissions). Attack Vector: Adjacent (closed hospital network zone; remote access, where permitted at all, only through the hospital's own infrastructure). User Interaction: Required (a user opens the affected form, report or profile). Scope: Changed (code runs on the user's workstation). The CNA record currently shows PR:L and AV:N (9.0); Mesalvo has requested correction.
Temporal (Mesalvo)	CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H/E:P/RL:T/RC:C – 7.2 (High). E:P: demonstrated in a security test; no exploit code public. RL:T: vendor guidance available (this advisory). RC:C: confirmed.
Environmental	Note for operators: workstation application control (recommended in MSA-2026-001) does not reduce this score, because scripts execute inside the signed MEONA Client process. The relevant environmental controls are permission governance and audit-log review. Operators should compute their own Environmental score.

Recommendations for operators

- Assign USER_DEFINED_FORMS_ADMINISTRATOR, SPRING_ADMINISTRATOR, XML_CONTENT_EDITOR and XML_ARCHIVER_EDITOR, as well as the administrative roles that open the administration area, only to a small, named group of administrators, under the same approval and review process as workstation or domain administrator rights.
- Review the assignment of the administrative roles that grant access to the administration area (ADMINISTRATOR, SUPERADMINISTRATOR, TYPIST for catalogue editing, or PHARMACIST with the PHARMACY_ADMINISTRATOR right) with the same care, since any of them permits editing of the Spring.NET XML categories OBJECT_DEFINITION and APPLICATION_EDITOR_REGISTRY.
- Review the assignments of these permissions now and at regular intervals; remove them from accounts that do not need them, including service and shared accounts.
- Apply a four-eyes principle to the creation and modification of scripts and Spring XML configurations; test changes on the test system before activating them for productive profiles.
- Review the MEONA Server audit log for changes to scripts and Spring XML configurations and reconcile them with approved change requests.
- 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 functions described are 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 workstations. 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 describes the functions as a code-injection vulnerability exploitable with low privileges over the network (CVSS 9.0). Mesalvo has requested under the CVE Program dispute policy that the record be rejected as describing intended administrative functionality or, alternatively, corrected to state the administrative permissions required, the documented nature of the functions, the closed network deployment and the corresponding 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 scripting and configuration functions are documented administrative functions restricted to explicitly assigned administrative permissions, and their use by a permission holder is not a weakness of the product. 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-2026-22314
- NVD: https://nvd.nist.gov/vuln/detail/CVE-2026-22314
- MSA-2026-001 (CVE-2026-0856), MSA-2026-004 (CVE-2026-22315)
- MEONA Konfigurationsanleitung 2025.04, Version 1.0 (21 September 2026; UDI-DI 4262357191084): "Benutzerdefinierte Formulare" incl. "Skripte" (pp. 253–254), "Benutzerdefiniertes Reporting" (p. 259 ff.), security notice on separation of administrative and end-user duties (p. 39), appendices "Skripte", "Reporting" and "Spring XML"; earlier MEONA administration handbook, sections 11.9, 45.2.6, 48.1.1.2, 48.1.2.12, 48.1.4
- 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 scripting, reporting and Spring XML documentation as appendices. No change to the assessment.