**Mesalvo Security Advisory**

# MSA-2026-005: Client-supplied recipient address in the MEONA feedback function (CVE-2026-25602)

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-2026-005.pdf

| | |
|---|---|
| **Advisory ID** | MSA-2026-005 |
| **CVE** | CVE-2026-25602 (CNA: ENISA). Mesalvo has requested correction of the record's description, affected versions and CVSS vector. |
| **Published / last updated** | 21 September 2026 / 21 September 2026 – Version 1.0 |
| **Severity** | CVSS v3.1 Base 2.3 (Low) per Mesalvo assessment (the CNA record shows 4.4 pending correction). Temporal 2.1 (Low). |
| **Status** | Product change planned for a MEONA release in 2027. Recommended mail-relay configuration 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

The MEONA feedback function in the administration area lets users with an administrative role send a feedback report by e-mail to a configured mailbox. The recipient address is transmitted by the MEONA Client, and the MEONA Server uses the transmitted address. Such a user who modifies the request can have the server send a message with content of their choosing, from the internal MEONA sender address, to a recipient of their choosing, within the limits of the hospital's mail relay. Such a message can be used for social engineering because it appears to come from an internal system. MEONA will use the configured recipient address on the server side; until then operators can restrict the MEONA sender address at their mail relay.

## Products and versions concerned

MEONA Client and MEONA Server, versions 2024.10, 2025.04 and 2026.03. Changed in a MEONA release in 2027.

## Description

When a user submits a feedback report (administration area → Kommunikation → Feedback Report), the MEONA Client sends recipient, subject and text to the MEONA Server, which sends the e-mail through the hospital's SMTP relay from the sender address configured in the server setting CLIENT_FAILURE_SENDER (default noreply@meona.de). The server does not verify the recipient address against its own configuration. A user who alters the request can therefore choose the recipient. The message contains only the recipient, subject and text entered by the user; no data of other users or patients is disclosed by the weakness. Mesalvo classifies it as CWE-345 (Insufficient Verification of Data Authenticity).

## Conditions under which the behaviour can be misused

1. A MEONA account with one of the administrative roles that grant access to the administration area (ADMINISTRATOR, SUPERADMINISTRATOR, TYPIST for catalogue editing, or PHARMACIST with the PHARMACY_ADMINISTRATOR right), assigned explicitly by the hospital's administrators.
2. Access to the hospital's internal network. 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. A mail relay that delivers messages from the MEONA sender address to the chosen recipient. Where the relay restricts the sender address to the configured feedback mailbox or to internal domains, external recipients cannot be reached.

## Effect on information security

A message with content chosen by the sender sent from a trusted internal address, usable for phishing or social engineering against the recipients. No information is disclosed to the sender and no data is modified in MEONA.

## CVSS

| | |
|---|---|
| **Base (Mesalvo)** | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N – 2.3 (Low). The CNA record shows C:L and PR:L (4.4); Mesalvo has requested correction to C:N, because the person obtains no information through the weakness, and to PR:H, because the function requires an administrative role. |
| **Temporal (Mesalvo)** | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N/E:P/RL:W/RC:C – 2.1 (Low). E:P: demonstrated in a security test. RL:W: operator configuration at the mail relay; product change pending. RC:C: confirmed. |
| **Environmental** | Operators whose mail relay restricts the MEONA sender address to the configured feedback mailbox have removed the external delivery path and may score the integrity impact as None for their environment. |

## Product change

A MEONA release in 2027 will use a recipient address configured on the MEONA Server for feedback reports and ignore any recipient transmitted by the client.

## Recommended operating configuration (until the product change is installed)

- Configure the hospital's mail relay so that messages from the MEONA sender address are delivered only to the configured feedback mailbox (or, at minimum, only to internal domains), and reject or quarantine messages from that address to other recipients.
- Monitor the relay log for messages from the MEONA sender address to unexpected recipients.
- Include the MEONA sender address in staff awareness material: feedback confirmations never ask for credentials or actions.

## 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 planned product change is a security hardening of the feedback function delivered in a regular release; it does 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.

## 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 privileges required and the severity; Mesalvo did accept that the recipient address should be determined on the server side. Mesalvo did not agree to the publication of this record in its published form. The record was published by the CNA on 20 May 2026; 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 record against the product facts and the scheduling of the related product change. 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-2026-25602
- NVD: https://nvd.nist.gov/vuln/detail/CVE-2026-25602
- Mesalvo Vulnerability Disclosure Policy: https://mesalvo.com/en/vdp

## Revision history

| Version | Date | Change |
|---|---|---|
| 1.0 | 21 September 2026 | Initial publication. |