Mesalvo Security Advisory

MSA-2026-002: Legacy password storage methods for accounts predating MEONA 2024.10 (CVE-2026-0857)

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-2026-002.pdf

Advisory ID	MSA-2026-002
CVE	CVE-2026-0857 (CNA: ENISA). Mesalvo has requested correction of the record; the published record describes the weakness inaccurately (see "Note on the CVE record").
Published / last updated	21 September 2026 / 21 September 2026 – Version 1.0
Severity	CVSS v3.1 Base 4.4 (Medium) per Mesalvo assessment (the CNA record shows 6.0 pending correction). Temporal 4.0 (Medium).
Status	Product change in the regular service packs MEONA 2025.04.24 and 2026.03.02 (Q4 2026). Recommended operating configuration available now. Installations in which every password has been set or changed under MEONA 2024.10 or later are not affected.
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

Since MEONA 2024.10 (June 2024) MEONA protects stored user passwords with Argon2, and every password that is set or changed is stored with Argon2. Earlier versions protected passwords with SHA-1 (from October 2015) or stored them without protection (before). Passwords last set under an earlier version keep the earlier method until they are changed, and a MEONA super administrator can read the stored value of such accounts in the user administration. Only accounts managed locally in MEONA are affected; users authenticated through the hospital's directory service have no password stored in MEONA. MEONA 2025.04.24 and 2026.03.02 remove the legacy methods, force a new password for every affected account and stop displaying stored values.

Products and versions concerned

Product	Versions	Status
MEONA Server / MEONA Client	2024.10, all service packs	Applies to local accounts with passwords last set under earlier versions. End of support; apply the recommended operating configuration.
MEONA Server / MEONA Client	2025.04, service packs before 2025.04.24	Applies to such accounts. Changed in 2025.04.24 (Q4 2026).
MEONA Server / MEONA Client	2026.03, service packs before	Applies to such accounts. Changed in

Product	Versions	Status
	2026.03.02	2026.03.02 (Q4 2026).

Description

MEONA stores user passwords in its database. The storage method changed twice: from unprotected storage to SHA-1 hashing in October 2015, and from SHA-1 to Argon2 with MEONA 2024.10 in June 2024. A password is stored with the method in force when it is set or changed; passwords last set under an earlier version therefore keep SHA-1 or, for accounts untouched since 2015, remain unprotected until the user changes them. The user administration also allowed an administrator to select the storage method per account. SHA-1 hashes of typical passwords can be recovered with modest effort, and an unprotected value can be read directly. The user administration of the MEONA Client displays the stored value to super administrators, and it can be exported through the administrative database functions (see MSA-2026-004 / CVE-2026-22315). The weakness concerns only accounts managed locally in MEONA: accounts authenticated through the hospital's directory service (Active Directory / Entra ID) have no password stored in MEONA. In typical installations end users authenticate through the directory service and local accounts are limited to emergency accounts, which are normally disabled and enabled only when needed, and technical accounts. Mesalvo classifies the weakness as CWE-916 (Use of a Password Hash With Insufficient Computational Effort).

Conditions under which the behaviour can be misused

1. At least one locally managed user account whose password was last set under a version before MEONA 2024.10 (or for which an administrator selected a legacy method). Installations in which every local password has been set or changed under 2024.10 or later, and accounts authenticated through the directory service, are not affected.
2. Super administrator permissions in MEONA, or direct access to the MEONA database. The security test reached these permissions by way of CVE-2026-0856 (see MSA-2026-001).
3. 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.

Effect on information security

Disclosure of the passwords of affected local accounts to a MEONA super administrator. Where users reuse passwords across systems, disclosed passwords may be tried against other systems; this is a consequence of password reuse and is addressed by the operator recommendations below.

CVSS

Base (Mesalvo)	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N – 4.4 (Medium). The CNA record currently shows S:C (6.0); Mesalvo has requested correction to S:U, because the disclosed data are MEONA's own stored credentials and no other security authority is affected by the weakness itself.
Temporal (Mesalvo)	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:T/RC:C – 4.0 (Medium). E:P: demonstrated in a security test, no exploit code public. RL:T: operating configuration recommendation available now; product change in the Q4 2026 service packs. RC:C: confirmed.
Environmental	Operators whose users have all changed their password since the upgrade to

	MEONA 2024.10 are not affected (Modified Confidentiality: None → Environmental 0.0). For affected operators the Environmental score depends chiefly on the Confidentiality Requirement; with CR:H it is 5.6. Operators should compute their own score with the FIRST CVSS v3.1 calculator.

How to check whether you are affected

Any locally managed account whose password has not been changed since the installation of MEONA 2024.10 is affected. The stored method is recorded per account and can be listed in two ways.

- For all local accounts at once: in the MEONA administration area, Spezielle Reports → SQL-Abfragen (permission REPORT_GLOBAL), run the following query. It covers every local account, including emergency and maintenance accounts. The same query can be run directly against the MEONA database by the database administrator.

```
SELECT user_name, first_name, last_name, password_protection FROM generic_user WHERE password_protection IN ('PLAINTEXT', 'MD5', 'SHA1');
```

- For a single account: Benutzer und Rechte → Lokale Benutzer → open the account; the field Passwortverschlüsselung shows the stored method (Argon2, SHA1, MD5 or Klartext).

Accounts whose password_protection is ARGON2 are not affected. Accounts authenticated through the directory service do not appear in this table with a password.

Product change

MEONA 2025.04.24 and 2026.03.02 (planned Q4 2026) remove the legacy storage methods from the user administration, require every account still stored with a legacy method to set a new password at next logon, which is then stored with Argon2, and no longer display stored credential values in the user administration. The change completes the migration to Argon2 begun with MEONA 2024.10; it does not alter the clinical functions or the intended purpose of MEONA.

Recommended operating configuration (until the service packs are installed)

- Force a password change at next logon for all local accounts listed by the check above; the new password is stored with Argon2. For emergency accounts that are kept disabled, set a new password when they are next enabled, or set it now and keep them disabled.
- Do not select a legacy storage method for any account.
- Restrict super administrator permissions to the smallest possible group and review the assignments.
- Where MEONA is integrated with the hospital's central identity provider (Active Directory / Entra ID), prefer central authentication so that MEONA stores no passwords for those accounts.
- Remind users that passwords must not be reused across systems; where reuse is suspected for affected accounts, rotate the passwords on the other systems as well.

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 change described above completes the migration of password storage to Argon2 that began with MEONA 2024.10 and is delivered in the regular service packs; 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.

Note on the CVE record

The CVE record as published by the CNA on 20 May 2026 names CWE-316 (cleartext storage of sensitive information in memory) and contains no description of attacker, prerequisites or impact. The weakness named in the record (CWE-316) is not present in MEONA; the weakness described in this advisory (CWE-916, legacy password storage methods of local accounts) is, and Mesalvo does not dispute it. Mesalvo has requested correction of the classification, description, affected products and versions, remediation information, references and CVSS vector under the CVE Program dispute policy and will update this advisory when the record is corrected.

Coordination and disclosure

Mesalvo replaced SHA-1 by Argon2 as the default password storage method in MEONA 2024.10, released in June 2024, and announced the change in the release notes. 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 classification, the accounts concerned (locally managed accounts only), the conditions for misuse and the severity; Mesalvo did agree that the legacy storage methods should be documented in a CVE record with a corrected description. In the discussion of 4 May 2026 Mesalvo therefore agreed to a CVE record for this finding subject to its approval of the text. The record was 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 record against the product facts and the scheduling of the related product change 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-2026-0857
- NVD: https://nvd.nist.gov/vuln/detail/CVE-2026-0857
- MEONA 2024.10 release notes, "Secure Password Storage"
- MSA-2026-001 (CVE-2026-0856), MSA-2026-004 (CVE-2026-22315)
- Mesalvo Vulnerability Disclosure Policy: https://mesalvo.com/en/vdp

Revision history

Version	Date	Change
1.0	21 September 2026	Initial publication.