NEWS / 30. 3. 2026

# CVE-2026-25601 – Credential Exposure vulnerability in MEPIS RM

## Summary

A vulnerability was identified in MEPIS RM, an industrial software product developed by Metronik. The application contained a hardcoded cryptographic key within the Mx.Web.ComponentModel.dll component. When the option to store domain passwords was enabled, this key was used to encrypt user passwords before storing them in the application's database. An attacker with sufficient privileges to access the database could extract the encrypted passwords, decrypt them using the embedded key, and gain unauthorized access to the associated ICS/OT environment.

## Identifiers

**CVE-2026-25601**
*Vendor:* **Metronik d.o.o.**
*Product:* **MEPIS RM** (https://mepis.eu/solutions/mepis-rm/)
*Vulnerability:* **Hard-coded secret keys stored in a DLL library** (Credential Exposure)
*CVSS score:* **6.4** (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H)
***CWE-798:*** **Use of Hardcoded Credentials**

## Vulnerable products

Affected Versions

- MEPIS RM 8.0.0007 — vulnerable; no longer deployed at customer sites
- MEPIS RM 8.1.0007 — vulnerable; no longer deployed at customer sites
- MEPIS RM 8.2.0007 (up to build 14) — vulnerable due to the hard-coded secret key in the MxWebServer component
- MEPIS RM 8.2.0007 build 15 — not vulnerable; the issue is fixed in this component build
- MEPIS RM 8.2.0107 — product version that will include the fully integrated fix

The vulnerability is effectively resolved starting with MEPIS RM 8.2.0007 build 15, with the final consolidated fix delivered in MEPIS RM 8.2.0107.

## Details

The vulnerability is reflected in the use of a hard-coded secret key within the *MxWebServer* component of *MEPIS RM*. When the password storage functionality was enabled,this component was used to encrypt passwords before storing them in the system. Because the key was embedded directly in the DLL, an attacker with sufficient access to the application environment or database could extract encrypted credentials and decrypt them offline, potentially gaining unauthorized access to *ICS/OT* systems integrated with *MEPIS RM*. The issue affects legacy versions *8.0.0007* and *8.1.0007*, as well as *MEPIS RM 8.2.0007* up to *build 14*, where the vulnerable component was still in use. Metronik has implemented a corrected password-handling mechanism in *MEPIS RM 8.2.0007 build 15*, and the fully integrated product-level fix will be delivered in *MEPIS RM 8.2.0107*. The vendor notes that exploitation requires local access, which is not typical in customer deployments, and is currently coordinating safe rollout of the fix due to the operational constraints of production environments.

## Impact

The hard-coded secret key in the *MxWebServer* component allows an attacker with local or database-level access to decrypt stored credentials, weakening authentication controls in environments where *MEPIS RM* is deployed. With decrypted credentials, an attacker could gain unauthorized access to connected *ICS/OT* systems, potentially enabling manipulation of industrial processes, operational disruption, or lateral movement within critical infrastructure networks. Although the vendor notes that exploitation requires local access, which is not typical in customer deployments, the vulnerability still represents a meaningful security risk in production environments.

## Exploitation status

There are currently no known exploits in circulation that target this vulnerability.

## Mitigation

The vulnerability is addressed in *MEPIS RM 8.2.0007 build 15*, and the fully integrated product-level fix will be delivered in *MEPIS RM 8.2.0107*. Upgrading to these versions removes the hard-coded key and introduces secure password-handling mechanisms.

## Timeline

- 15 January 2026 — Initial report submitted to SI-CERT regarding the possibility of vulnerable Metronik products.
- 21 January 2026 — Vulnerability researcher provided detailed technical information about the identified issues.
- 3 February 2026 — Vendor formally notified of the vulnerability.
- 4 February 2026 — Vendor confirmed the vulnerability and began internal remediation activities.
- 31 March 2026 — Advisory published

## Acknowledgments

The vulnerability was identified and responsibly disclosed by **Mijo Mišić**, penetration tester at *Combis d.o.o.*, Croatia, whose analysis enabled the vendor to confirm the issue and implement a fix.

## Contact

SI-CERT

ARNES
Tehnološki park 18, 1000 Ljubljana

T: 01 479 88 00
E: info@cert.si

## READ ALSO

NEWS / 24. 2. 2026
### VANTAGE – Vulnerability Assessment aNd Testing Automation for Global Enhancement

Project coordinator Diadikasia Business Consulting Symvouloi Epicheiriseon AE Diadikasia Business Consultants SA, GR Project partners Project duration 1 January 2026 – 31 December 2028 (36 months) Summary VANTAGE (Vulnerability Assessment ...

MORE →

EU PROJEKTI,NEWS / 21. 1. 2025
### INTERCEPT – IncideNt ThrEat shaRing CybErsecurity PlaTform

Project coordinator: T-2, Družba za ustvarjanje razvoj in trženje elektronskih komunikacij in opreme d. o. o., Slovenia Contact details: intercept@t-2.com Project partners: T-2 d. o. o., Družba za ustvarjanje ...

MORE →

EU PROJEKTI,NEWS / 21. 1. 2025
### CyberSEAS: Cyber Securing Energy dAta Services

The CyberSEAS project is a collaborative project improving the cyber security of the European electrical power energy systems (EPES) and the overall resilience of energy supply chains, protecting them from ...

MORE →