Safety Advisory / CVE Report

Document Revision **1.1** dated 09.09.2026

All rights reserved. © IEP GmbH 1996-2026

Revision History

Rev.	Date	Name	Change
1.1	09.09.2026	HK	CVE-2026-00001
1.0	19.05.2026	HK	Initial Version

Contents

1 Introduction 1
1.1 Fictive Example CVE-2026-XXXXX 1
2 Common Vulnerabillities and Exposures (CVE) 2
2.1 CVE-2026-00001 2
3 EU Cyber Resilience Act (CRA) Compliance 3
3.1 Cryptographic Integrity of Software, Firmware, and Updates 4

1 Introduction

This document summarizes Common Vulnerabilities and Exposures (**CVE**) affecting IEP GmbH software and hardware products. Beyond individual CVE disclosures, it provides guidance on the compliance implications of applicable cybersecurity regulations for IEP products, including the EU Cyber Resilience Act (CRA), discussed in Sect. 3. All CVEs are documented in Sect. 2.

This document serves as the sole authoritative source for CVE disclosures relating to IEP products and will be updated on a rolling basis as new vulnerabilities are identified and remediated. Vulnerability reports and associated fixes follow the format illustrated in the example below.

1.1 Fictive Example CVE-2026-XXXXX

CVE ID	CVE-2026-XXXXX
Severity	CRITICAL
Affected Product	FAKE RTOS-UH
Affected Versions	v1.0.0 – v1.2.1
Fixed Version	v2.4.2
Published	2026-05-04
Last Updated	2026-05-04
Reporter	Hermann Kroll (IEP)

A Telnet server is always started with a default user and password. Attackers could login via Telnet and execute arbitrary code. The vulnerability affects all running RTOS-UH devices with a network configuration.

⚠ **Action Required:** Upgrade to **v2.4.2** immediately. This version will deactivate the default user and password. Users must explicitly set custom users and passwords when working with Telnet. A guide to update RTOS-UH can be found here.

Users need to set a Telnet user and password.

Listing 1: Step-by-Guide to set Telnet users

```
// Set your Telnet user and password
WORD /FD/TELNET.cred
// User: Hermann, Password: Kroll
// Restart your device via
VME_RESET
```

2 Common Vulnerabillities and Exposures (CVE)

2.1 CVE-2026-00001

CVE ID	CVE-2026-00001
Severity	MEDIUM
Affected Product	RTOS-UH - CanLib
Affected Versions	v1.0 – v7.9
Fixed Version	v8.0
Published	2026-09-09
Last Updated	2026-09-09
Reporter	Hermann Kroll (IEP)

CAN-FD or tampered/faulty CAN packets (that do not comply with the standard) may cause RTOS-UH to crash under certain circumstances. CANLib version 8.0 and later resolves this issue and prevents system crashes.

Either update the CanLib or control that your CAN participants comply to the official standard and that no CAN-FD participants are present.

3 EU Cyber Resilience Act (CRA) Compliance

IEP GmbH is committed to ensuring that all current and future software and hardware products meet the requirements set forth by the EU Cyber Resilience Act (Regulation (EU) 2024/2847), which entered into force on 11 December 2024 and will become fully applicable on 11 December 2027.

In accordance with the CRA, IEP GmbH undertakes the following obligations across its entire product portfolio:

- **Secure by Design:** All IEP products are developed in accordance with secure-by-design and secure-by-default principles, ensuring that cybersecurity is addressed throughout the entire product lifecycle — from initial design through decommissioning.
- **Vulnerability Management:** IEP GmbH maintains a vulnerability management process. Identified vulnerabilities are assessed, tracked, and remediated in a timely manner. CVE disclosures are published in accordance with coordinated disclosure practices, as detailed in Sect. 2.
- **Security Updates:** IEP GmbH commits to providing security patches and updates for its products for a minimum support period consistent with the expected product lifetime and CRA requirements, ensuring that known vulnerabilities are addressed without undue delay.
- **Incident Reporting:** In the event of an actively exploited vulnerability affecting an IEP product, IEP GmbH will notify affected customers and if required relevant national authority, in accordance with the reporting timelines prescribed by the CRA.
- **Conformity Assessment:** IEP products subject to mandatory third-party conformity assessment under the CRA will undergo the applicable assessment procedures prior to being placed on the EU market. A Declaration of Conformity and CE marking will be issued accordingly.
- **Software Bill of Materials (SBOM):** IEP GmbH maintains an up-to-date Software Bill of Materials for its products, enabling transparent identification of all software components and their respective versions, including third-party and open-source dependencies.

IEP GmbH continuously monitors regulatory developments and guidance issued by the European Commission, ENISA, and relevant standardisation bodies (including ETSI and CEN/CENELEC) to ensure ongoing compliance as implementing acts and harmonised standards are published. Any updates to IEP's compliance posture will be reflected in subsequent revisions of this document.

For questions regarding IEP GmbH's CRA compliance program, please contact the IEP Security Team at security@iep.de.

3.1 Cryptographic Integrity of Software, Firmware, and Updates

IEP GmbH employs cryptographic signing and encryption for all software, firmware, and update packages distributed to customers. This ensures the authenticity, integrity, and confidentiality of all IEP deliverables and protects against unauthorised modification, tampering, or supply chain attacks. IEP GmbH provides tools for RTOS-UH and Windows to check the integrity and decrypt certain files when necessary.

Asymmetric Key Infrastructure

All IEP software, firmware, and update artifacts are signed using asymmetric cryptography based on a dedicated IEP Code Signing infrastructure. The following standards and algorithms are employed in accordance with established recommendations:

- **Digital Signatures:** All release artifacts are signed using RSA signatures with a minimum key length of **4096 bits**.
- **Key Management:** IEP GmbH stores private keys exclusively on dedicated hardware and never shares these keys.
- **Certificate Authority:** IEP operates an internal **PKI (Public Key Infrastructure)** with a dedicated offline **Root CA** and one or more intermediate **Code Signing CAs**. Certificates are issued in accordance with **X.509 v3** and follow typical validity periods and revocation practices.
- **Encryption of Update Packages:** Where confidentiality of update content is required, packages are encrypted using **AES-256**, providing both encryption and authenticated integrity verification.
- **Hash Integrity:** In addition to digital signatures, all artifacts are accompanied by a **SHA-256** or **SHA-512** manifest file, enabling independent integrity verification by customers and auditors.
- RTOS-UH receives additional tools to verify the integrity of software before execution.

Signature Verification by Customers

Customers are strongly advised to verify the cryptographic signature of all IEP software and firmware packages prior to installation. IEP shares its current public signing certificates with corresponding customers. IEP will generate a dedicated key pair for each customer.

A detached signature file (`.sig`) and a SHA-256 checksum file (`.sha256`) accompany every release artifact. Verification can be performed using standard tooling, for example:

Listing 2: Signature and integrity verification

```
# Verify SHA-256 checksum
sha256sum --check firmware-v1.2.3.bin.sha256

# Verify digital signature using the IEP public key
openssl dgst -sha256 -verify iep-codesign.pub.pem \
    -signature firmware-v1.2.3.bin.sig \
    firmware-v1.2.3.bin
```

Key Rotation and Revocation

IEP code signing keys are rotated on a regular basis in accordance with BSI recommendations. In the event that a signing key is compromised or suspected of compromise, IEP will:

1. Immediately revoke the affected certificate via the IEP **Certificate Revocation List (CRL)**.
2. Re-sign all current release artifacts with the new key.
3. Notify all registered customers and publish a security notice in this document.
4. Issue a CVE or security advisory if the compromise has any downstream impact on deployed products.

Customers are advised to configure their systems to check the IEP endpoint prior to trusting any IEP-signed artifact, particularly in high-security or safety-critical deployment environments.