# Sicherheitsdokument / CVE Report

Dokument-Revision **1.0** vom 07.05.2026

# Revisionshistorie

| Rev. | Datum | Name | Änderung |
|---|---|---|---|
| 1.0 | 19.05.2026 | HK | Erstellung |

# Inhaltsverzeichnis

# 1 Einleitung

Dieses Dokument fasst die Common Vulnerabilities and Exposures (**CVE**) zusammen, die Software- und Hardwareprodukte der IEP GmbH betreffen. Über die einzelnen CVE-Offenlegungen hinaus bietet es Leitlinien zu den Auswirkungen der geltenden Cybersicherheitsvorschriften auf die Konformität von IEP-Produkten. Der EU Cyber Resilience Act (CRA) wird in Abschnitt 3 behandelt wird. Alle CVEs sind in Abschnitt 2 dokumentiert.

Dieses Dokument dient als einzige maßgebliche Quelle für CVE-Offenlegungen in Bezug auf IEP-Produkte und wird fortlaufend aktualisiert, sobald neue Sicherheitslücken identifiziert und behoben werden. Sicherheitslückenberichte und die dazugehörigen Korrekturen folgen dem im folgenden Beispiel dargestellten Format.

## 1.1 Fiktives Beispiel CVE-2026-XXXXX

| | |
|---|---|
| **CVE-ID** | CVE-2026-XXXXX |
| **Interne ID** | IEP-2026-001 |
| **Schweregrad** | CRITICAL |
| **Betroffenes Produkt** | FAKE RTOS-UH |
| **Betroffene Versionen** | v1.0.0 – v1.2.1 |
| **Behobene Version** | v2.4.2 |
| **Veröffentlicht** | 04.05.2026 |
| **Letzte Aktualisierung** | 04.05.2026 |
| **Meldender** | Hermann Kroll (IEP) |

Ein Telnet-Server wird immer mit einem Standardbenutzer und einem Standardpasswort gestartet. Angreifer könnten sich über Telnet anmelden und beliebigen Code ausführen. Die Sicherheitslücke betrifft alle laufenden RTOS-UH-Geräte mit einer Netzwerkkonfiguration.

⚠ **Erforderliche Maßnahme:** Führen Sie unverzüglich ein Update auf **v2.4.2** durch. Diese Version deaktiviert den Standardbenutzer und das Standardpasswort. Benutzer müssen bei der Arbeit mit Telnet explizit eigene Benutzer und Passwörter festlegen. Eine Anleitung zum Aktualisieren von RTOS-UH finden Sie hier.

Benutzer müssen einen Telnet-Benutzer und ein Passwort festlegen.

Listing 1: Schritt-für-Schritt-Anleitung zum Einrichten von Telnet-Benutzern

```
// Legen Sie Ihren Telnet-Benutzer und Ihr Passwort fest
WORD /FD/TELNET.cred
// Benutzer: Hermann, Passwort: Kroll
// Neustarten
VME_RESET
```

# 2 Common Vulnerabillities and Exposures (CVE)

# 3 Einhaltung des EU-Gesetzes zur Cyber-Resilienz (CRA)

IEP GmbH verpflichtet sich sicherzustellen, dass alle aktuellen und zukünftigen Software- und Hardwareprodukte die Anforderungen des EU Cyber Resilience Act (Verordnung (EU) 2024/2847) erfüllen, der am 11. Dezember 2024 in Kraft getreten ist und am 11. Dezember 2027 vollständig umgesetzt werden muss.

In Übereinstimmung mit dem CRA übernimmt die IEP GmbH für ihr gesamtes Produktportfolio die folgenden Verpflichtungen:

- **Secure by Design:** Alle IEP-Produkte werden nach den Prinzipien „Secure by Design“ und „Secure by Default“ entwickelt, wodurch sichergestellt wird, dass die Cybersicherheit während des gesamten Produktlebenszyklus berücksichtigt wird – vom ersten Entwurf bis zur Außerbetriebnahme.
- **Schwachstellenmanagement:** IEP GmbH unterhält einen Schwachstellenmanagementprozess. Identifizierte Schwachstellen werden bewertet, nachverfolgt und zeitnah behoben. CVE-Offenlegungen werden gemäß den koordinierten Offenlegungspraktiken veröffentlicht, wie in Abschnitt 2 beschrieben.
- **Sicherheitsupdates:** IEP GmbH verpflichtet sich, Sicherheitspatches und Updates für ihre Produkte über einen Mindest-Supportzeitraum bereitzustellen, der der erwarteten Produktlebensdauer und den CRA-Anforderungen entspricht, um sicherzustellen, dass bekannte Sicherheitslücken unverzüglich behoben werden.
- **Meldung von Vorfällen:** Im Falle einer aktiv ausgenutzten Sicherheitslücke, die ein IEP Produkt betrifft, benachrichtigt die IEP GmbH die entsprechenden Kunden, und wenn benötigt, die zuständigen nationalen Behörden.
- **Konformitätsbewertung:** IEP Produkte, die einer obligatorischen Konformitätsbewertung durch Dritte gemäß der CRA unterliegen, durchlaufen die entsprechenden Bewertungsverfahren, bevor sie in der EU in Verkehr gebracht werden. Eine Konformitätserklärung und eine CE-Kennzeichnung werden entsprechend ausgestellt.
- **Software-Stückliste (SBOM):** Die IEP GmbH führt eine aktuelle Software und Firmwareliste für ihre Produkte, die eine transparente Identifizierung aller Softwarekomponenten und ihrer jeweiligen Versionen ermöglicht, einschließlich Abhängigkeiten von Drittanbietern und Open-Source-Komponenten.

IEP GmbH beobachtet kontinuierlich die regulatorischen Entwicklungen und Leitlinien, die von der Europäischen Kommission herausgegeben werden, um die fortlaufende Einhaltung der Vorschriften zu gewährleisten, sobald entsprechende Regeln, Gesetze oder Normen veröffentlicht werden. Alle Aktualisierungen der Compliance-Situation der IEP GmbH werden in nachfolgenden Überarbeitungen dieses Dokuments berücksichtigt.

Bei Fragen zum CRA-Compliance-Programm der IEP GmbH wenden Sie sich bitte an das IEP-Sicherheitsteam unter security@iep.de.

## 3.1 Kryptografische Integrität von Software, Firmware und Updates

Die IEP GmbH setzt kryptografische Signaturen und Verschlüsselung für alle Software-, Firmware- und Update-Pakete ein, die an Kunden verteilt werden. Dies gewährleistet die Authentizität, Integrität und Vertraulichkeit aller IEP-Lieferungen und schützt vor unbefugten Änderungen, Manipulationen oder Angriffen auf die Lieferkette. Die IEP GmbH stellt Tools für RTOS-UH und Windows bereit, um die Integrität zu überprüfen und bestimmte Dateien bei Bedarf zu entschlüsseln.

### Asymmetrische Schlüsselinfrastruktur

Alle IEP-Software-, Firmware- und Update-Artefakte werden mithilfe asymmetrischer Kryptografie auf Basis einer dedizierten IEP-Code-Signing-Infrastruktur signiert. Die folgenden Standards und Algorithmen werden in Übereinstimmung mit etablierten Empfehlungen verwendet:

- **Digitale Signaturen:** Alle Release-Artefakte werden mit RSA-Signaturen mit einer Mindestschlüssellänge von **4096 Bits** signiert.
- **Schlüsselverwaltung:** Die IEP GmbH speichert private Schlüssel ausschließlich auf dedizierter Hardware und gibt diese Schlüssel niemals weiter.
- **Zertifizierungsstelle:** Die IEP betreibt eine interne **PKI (Public Key Infrastructure)** mit einer dedizierten Offline- **Root CA** und einer oder mehreren intermediären **Code Signing CAs**. Zertifikate werden gemäß **X.509 v3** ausgestellt und unterliegen den üblichen Gültigkeitsfristen und Sperrverfahren.
- **Verschlüsselung von Update-Paketen:** Wenn die Vertraulichkeit der Update-Inhalte gewährleistet sein muss, werden die Pakete mit **AES-256** verschlüsselt, wodurch sowohl die Verschlüsselung als auch die authentifizierte Integritätsprüfung gewährleistet sind.
- **Hash-Integrität:** Zusätzlich zu digitalen Signaturen werden alle Artefakte von einer **SHA-256**- oder **SHA-512**-Manifestdatei begleitet, die eine unabhängige Integritätsprüfung durch Kunden ermöglicht.
- RTOS-UH erhält Tools zur Überprüfung der Softwareintegrität vor der Ausführung.

### Signaturüberprüfung durch Kunden

Kunden wird dringend empfohlen, die kryptografische Signatur aller IEP-Software- und Firmware-Pakete vor der Installation zu überprüfen. IEP versendet seine öffentlichen Signaturzertifikate an die jeweiligen Kunden. Für jeden Kunden wird ein eigenes Schlüsselpaar erzeugt.

Jedem Release-Artefakt liegen eine separate Signaturdatei (`.sig`) und eine SHA-256-Prüfsumme (`.sha256`) bei. Die Überprüfung kann mit Standardwerkzeugen durchgeführt werden, z.B.:

Listing 2: Signature and integrity verification

```
# SHA-256-Prüfsumme überprüfen
sha256sum --check firmware-v1.2.3.bin.sha256

# Digitale Signatur mit dem public IEP-Schlüssel überprüfen
openssl dgst -sha256 -verify iep-codesign.pub.pem \
    -signature firmware-v1.2.3.bin.sig \
    firmware-v1.2.3.bin
```

### Schlüsselrotation und -sperrung

IEP-Code-Signaturschlüssel werden gemäß den Empfehlungen des BSI regelmäßig rotiert. Falls ein Signaturschlüssel kompromittiert wurde oder der Verdacht auf eine Kompromittierung besteht, wird IEP GmbH:

1. Das betroffene Zertifikat unverzüglich über die IEP-Zertifikatssperrliste (CRL) widerrufen.
2. Alle aktuellen Release-Artefakte mit dem neuen Schlüssel neu signieren.
3. alle registrierten Kunden benachrichtigen und eine Sicherheitsmitteilung in diesem Dokument veröffentlichen.
4. eine CVE oder einen Sicherheitshinweis herausgeben, falls die Kompromittierung Auswirkungen auf bereits bereitgestellte Produkte hat.

Kunden wird empfohlen, ihre Systeme so zu konfigurieren, dass sie den IEP-Endpunkt überprüfen, bevor sie einem von IEP signierten Artefakt vertrauen, insbesondere in hochsicheren oder sicherheitskritischen Bereitstellungsumgebungen.