Process Description: Vulnerability Handling

1 Introduction

Ensuring product and equipment safety is a top priority for INSEVIS. As a manufacturer of components for industrial automation technology, we are aware of the role our products play within a comprehensive safety concept for machines and production facilities.

The purpose of this document is to transparently outline our approach to security incidents and vulnerabilities and to strengthen our long-term collaboration with our customers, users, and partners. INSEVIS hereby provides users with a consistent, clear source of information to explain our procedures for handling security incidents and to effectively support them in managing security risks.

The INSEVIS Product Security Incident Response Team (PSIRT) centrally manages all vulnerability management activities. The PSIRT's primary goal is to minimize potential risks to our customers arising from IT security vulnerabilities and to ensure the long-term secure usability of all INSEVIS products, software solutions, and applications. The PSIRT serves as the central authority within the company for investigating, assessing, and disclosing security risks. It acts as the central reporting point for all reports of potential vulnerabilities or security incidents related to INSEVIS products.

Upon receiving a report, the team immediately deploys the necessary resources to analyze and validate the issue and take appropriate corrective action. To ensure a standardized process, INSEVIS PSIRT works closely with the **CERT@VDE Alliance**. This collaboration ensures a coordinated response and transparent disclosure (Coordinated Vulnerability Disclosure) of all externally identified product vulnerabilities.

The structured vulnerability handling and disclosure process is divided into the following **four phases**:

1. **Report:** Secure receipt and initial registration of the vulnerability report.
2. **Analysis:** Technical validation, risk assessment (e.g., via CVSS), and root cause analysis.
3. **Editing:** Development, testing, and deployment of security updates, patches, or workarounds.
4. **Disclosure:** Publication of security advisories and guidance for affected users.

2 Report

The process for reporting security vulnerabilities is open to any individual or organization without restriction. Reports can be submitted regardless of existing contractual relationships, the lifecycle status of the affected product (including end-of-life products), or the customer's status with INSEVIS.

INSEVIS expressly welcomes vulnerability reports from security researchers, industry groups, CERTs, partners, and all other external sources. Receiving reports does not require the signing of a non-disclosure agreement (NDA).
INSEVIS respects the interests of the reporting party, treats reports completely anonymously upon request, and commits to investigating any vulnerability for which a reasonable connection to INSEVIS products can be suspected.

To ensure customer safety, INSEVIS urges the reporting parties to take coordinated action (Coordinated Vulnerability Disclosure). An immediate, uncoordinated disclosure leads to a critical zero-day situation that unnecessarily puts our customers' equipment and systems at risk.
To submit a vulnerability report concerning an INSEVIS product, the following channels are available for contacting the INSEVIS PSIRT:

- **E-Mail:** psirt@insevis.de
- **Report from the coordination partner CERT@VDE:** https://cert.vde.com
  To ensure efficient processing and validation, please provide the following information:
- **Description of the vulnerability:** Detailed reports, including proof-of-concept (PoC), exploit code, or relevant network protocols (if available).
- **Product identification:** Please provide the exact name of the affected product, the model, and the firmware version.
- **Current level of awareness:** Information on whether the vulnerability has already been publicly discussed or disclosed.
- **Mention in the Advisory:** Express consent or refusal (or a request to remain anonymous) regarding the inclusion of the reporter's name in the official INSEVIS Security Advisory.

Email communication with the INSEVIS PSIRT can be encrypted. The relevant S/MIME and PGP keys, as well as further information about the PSIRT, are available at the following link https://www.INSEVIS.de/

2.1 Handling of the Contact Information of Those Who Submit Reports

Upon receipt of a validated vulnerability report, the reporting party's contact information—if not already on file—is entered into the internal reporting database. This data is stored and maintained in strict accordance with the provisions of the General Data Protection Regulation (GDPR). The contact information is used exclusively for direct communication and coordination with the reporter during the ongoing process. Contact information for reporters with whom there has been no active communication for a period of three years will be deleted

For more information on data protection at INSEVIS, please visit https://www.INSEVIS.de

3 Analysis and Verification

The INSEVIS PSIRT systematically investigates and analyzes every incoming report. This review is conducted regardless of the affected software version or the current status of the product lifecycle, provided that the product has not yet reached its defined "Last Day of Support" (LDoS).

IAs a first step, INSEVIS verifies the relevance and specific applicability of the reported vulnerability to INSEVIS products. If the available data is insufficient for unambiguous validation, the PSIRT requests additional technical information from the reporting party on a case-by-case basis.

3.1 Classification of Vulnerabilities

To ensure objective assessment and risk-based prioritization as part of the vulnerability management process, INSEVIS classifies identified security vulnerabilities using a qualitative rating scale (Low, Medium, High, Critical).

As a standard practice, INSEVIS takes the following parameters into account for a well-founded risk assessment:

- **Potential impacts:** The scope and extent of damage caused by the vulnerability to the system's integrity, availability, and confidentiality.
- **Level of public awareness:** Current state of knowledge regarding the security vulnerability among experts.
- **Exploit Availability:** Verifiable existence or publication of functional exploit code.
- **Volume of impact:** Anzahl und Verbreitung der im Feld eingesetzten INSEVIS-Produkte, welche diese Schwachstelle aufweisen.
- **Availability of alternatives to a patch:** The availability of effective, temporary mitigation measures or workarounds as an interim solution until a final patch is released.

4 Processing

The INSEVIS PSIRT addresses identified security vulnerabilities in close coordination with the relevant internal development teams. As a strategic partner, CERT@VDE is notified of the security issue at an early stage. It assists the INSEVIS PSIRT, as needed, with technical assessments and the preparation of official CVE (Common Vulnerabilities and Exposures) entries and security advisories.s.

Throughout the entire processing phase, the INSEVIS PSIRT maintains regular communication with the reporting party. This facilitates a transparent exchange of information regarding the current status and ensures that the manufacturer’s technical position is understood. Where appropriate, preliminary versions of software fixes or drafts of security advisories may be provided to the reporter for verification and review.

4.1 Remedial Measures (Remediation)

INSEVIS investigates high-priority security risks and strives to promptly patch or mitigate validated vulnerabilities. If the results of the technical analysis require a modification to the product, appropriate corrective measures are developed and prepared for rollout.

The timeline for releasing fixes depends on various factors. These include the severity of the vulnerability, the affected product, the current development cycle, the product lifecycle, and whether a fix can be implemented exclusively as part of a major release.

The remedies provided may take the following forms:

- **Software-/Firmware-Release:** Release of a new, updated version of the software or firmware.
- **Patch/Update:** Provision of a targeted software fix by INSEVIS.
- **Third-Party Instructions:** Instructions for Installing Updates or Patches from Suppliers and Third-Party Vendors.
- **Workaround:** Documented measures to effectively mitigate the vulnerability without changing the code.

Notwithstanding these procedures, INSEVIS does not guarantee a specific technical solution for every problem. It is expressly noted that, given technological or architectural constraints, not all identified problems can be fully resolved.

5 Disclosure

Validated vulnerabilities are disclosed in a structured manner through official INSEVIS Security Advisories via CERT@VDE, as well as through software release notes within the company's own communication channels. The choice of disclosure channel is primarily based on the risk assessment:

- **Severity level "High" or "Critical":** For these vulnerabilities, INSEVIS generally publishes a dedicated security advisory via the CERT@VDE platform..
- **Severity level "Low" or "Moderate":** These security vulnerabilities are documented and disclosed as a matter of course in the regular software release notes.

INSEVIS reserves the right to deviate from these guidelines on a case-by-case basis, provided that additional risk factors necessitate an alternative approach.

5.1 CVE Numbering

INSEVIS initiates the assignment of a CVE (Common Vulnerabilities and Exposures) identifier if a verified vulnerability is directly related to the source code or a specific implementation of INSEVIS. The CVE number is physically assigned by the responsible CVE Numbering Authority (CNA), CERT@VDE.

CVE identifiers are not definitively assigned and published for reported vulnerabilities until the vulnerability has been officially confirmed by INSEVIS in consultation with CERT@VDE, or until it has been verifiably determined to exist in a third-party component in use.

5.2 INSEVIS Safety Advisory

INSEVIS Security Advisories provide detailed technical information about security risks that directly affect NSEVIS products and require a firmware upgrade, a software patch, or other customer actions (e.g., implementing a workaround). The main publications are available on the official CERT@VDE website: `https://cert.vde.com/de/advisories/vendor/insevis`.

By default, an INSEVIS Security Advisory contains the following information:

- **Technical Description:** A detailed description of the security vulnerability, including the CVE reference and the specific CVSS classification.
- **Impact Matrix:** Clear identification of all affected products, models, and software and hardware versions.
- **Mitigationen:** Comprehensive information on mitigating factors, countermeasures, and temporary workarounds.
- **Bezugsquellen:** Direct links to download the provided firmware updates or patches.
- **Dank (Acknowledgement):** Subject to express consent, the reporting party will be named to acknowledge its contribution to improving product safety.

5.3 Software Release Notices

Software release notes are used to transparently document fixed vulnerabilities with low or medium severity. These product-specific documents provide customers with all relevant information regarding version changes, new features, fixed bugs, and, where applicable, associated CVE IDs.

The release notes are available directly on the INSEVIS website for each product.

5.4 Customer Notification

INSEVIS strives to proactively inform customers as soon as a functional workaround or a final software fix for a security vulnerability has been identified and verified. For lifecycle and patch management, INSEVIS relies on established customer notification processes. Depending on the severity, these may include direct communication with customers, the public release of a security advisory, or detailed entries in the software release notes via CERT@VDE.

These notifications are triggered after the PSIRT has successfully completed the vulnerability handling and disclosure process and confirmed the existence of valid corrective measures or coordinated release plans to address the vulnerabilities.

If INSEVIS PSIRT identifies active exploitation of a vulnerability in the field that leads to an acute increase in risk for INSEVIS customers, the publication of a security advisory will be expedited as part of the risk management process. Such an immediate notification may contain prioritized recommendations for action, even if a final software patch is not yet available at that time.

To ensure a targeted and effective information policy, INSEVIS uses the following primary communication channels, depending on the severity of the vulnerability:

- **Key Publication:** Official publication of security advisories via the CERT@VDE platform.
- **Newsletter mailing list:** Regular and event-based updates for subscribed professional and customer groups.
- **Direct Communication:** Targeted email notifications to customers and operators who have verifiably purchased the specific product in question.

Im Sinne einer optimalen Informationsbereitstellung behält sich INSEVIS das Recht vor, von Fall zu Fall strategische Ausnahmen von diesen Standardprozeduren zu machen, um die Transparenz und Reichweite der Kommunikation für ein bestimmtes Dokument situativ zu maximieren.