HEIDENHAIN

Our Coordinated Vulnerability Disclosure (CVD) Policy (September 2026)

Our commitment

The security of our products is a top priority at HEIDENHAIN. We have a systematic process for handling reported security vulnerabilities regarding our products, solutions, and IT infrastructure, and collaborate closely with anyone who reports vulnerabilities. Complying with, continuously monitoring, and implementing regulatory requirements, such as the EU Cyber Resilience Act (CRA), are an integral part of our cybersecurity management process.

The following guidelines explain how vulnerabilities can be reported and how we handle them.

Applicability

These guidelines apply to all products offered by HEIDENHAIN, regardless of whether they are subject to servicing agreements and regardless of their status within the product life cycle.

We welcome reports from any source: researchers, trade associations, CERTs, partners, or third parties. We do not require a confidentiality agreement as a condition for accepting reports.

If your report is about our **digital infrastructure** (e.g., our website or active services), please send us an email to security@heidenhain.com.

Information for security researchers

HEIDENHAIN will not take legal action against reporting individuals if the following conditions are met:

- No harm to individuals
- Testing only to the extent necessary to verify a vulnerability
- Testing on productive systems only with explicit authorization
- No impairment of availability (no DoS attacks), no social engineering, and no access to physical infrastructure
- Access only to the data required for demonstration purposes; no modification, deletion, or exfiltration of data
- Protection of the security and privacy of others
- Compliance with applicable laws
- Willingness to coordinate disclosure (no public disclosure before the expiry of a mutually agreed period)

We value your reports and their ability to help us quickly remediate problems.

Guidelines for security researchers

- Notify us as early as possible about actual or potential security problems.
- Use exploits only to the extent necessary to verify the vulnerability.
- Give us sufficient time to remediate the problem. We will publish significant and confirmed vulnerabilities through CERT@VDE.
- Immediate public disclosure would create a "zero-day" situation and would expose our customers' systems, including critical infrastructure, to unnecessary risks. We therefore strongly request coordinated disclosure.

Reporting a vulnerability

- To send a detailed vulnerability report, along with any related files and confirming evidence, please use our cybersecurity contact form.
- **Email:** product-security@heidenhain.com (The email addresses stated in our security.txt are intended solely for initial contact and are not to be used for sending sensitive or detailed information regarding vulnerabilities.)
- **Reporting through CERT@VDE:** https://www.certvde.com/en/service/report-a-vulnerability/

What the report should contain

If possible, please provide the following information:

- The affected product or software (including ID number and software or firmware version)
- Description of the vulnerability, where it was found, and its potential effects
- Any reproducible steps (PoC, scripts, screenshots, network data)
- Whether or not the vulnerability is already public knowledge
- Any relevant documents (CVE, notifications, release notes)
- Preferably a description in English

How we process reports

1. **Report received:** We provide confirmation that the report was received.
2. **Assessment:** We examine and reproduce the vulnerability, requesting more information if needed.
3. **Handling:** We coordinate remediation and keep you informed.
4. **Public disclosure:** As soon as a solution is available or has been published (whichever occurs first), we will publish a security advisory. CVE entries will be created in coordination with CERT@VDE and published in accordance with the CSAF.

What our security advisories contain

Our security advisory will usually contain the following information:

- A description of the vulnerability with a CVE reference and CVSS score
- Any affected products and versions
- Information about workarounds and risk-reducing measures
- Information about available updates/fixes

DR. JOHANNES HEIDENHAIN GmbH
Dr.-Johannes-Heidenhain-Straße 5
83301 Traunreut, Germany
☎ +49 8669 31-0
FAX +49 8669 32-5061
service@heidenhain.de

www.heidenhain.com

11/2026

HEIDENHAIN

Richtlinie zur koordinierten Offenlegung von Schwachstellen (September 2026)

Unser Commitment

Die Sicherheit unserer Produkte hat für HEIDENHAIN höchste Priorität. Wir haben einen strukturierten Prozess zur Behandlung gemeldeter Sicherheitslücken in unseren Produkten, Lösungen und unserer IT-Infrastruktur und arbeiten vertrauensvoll mit allen Personen zusammen, die uns Schwachstellen melden. Die Einhaltung, fortlaufende Beobachtung und Umsetzung regulatorischer Vorgaben – wie des EU Cyber Resilience Act (CRA) – sind ein integraler Bestandteil unseres Cyber-Security-Managements.

Diese Richtlinie gibt klare Hinweise dazu, wie Schwachstellen gemeldet werden können und wie wir damit umgehen.

Geltungsbereich

Diese Richtlinie gilt für alle von HEIDENHAIN angebotenen Produkte – unabhängig von bestehenden Serviceverträgen oder dem Lebenszyklusstatus eines Produkts.

Wir begrüßen Meldungen von jeglichen Quellen: Forschenden, Branchenorganisationen, CERTs, Partnern oder anderen Dritten. Eine Geheimhaltungsvereinbarung ist keine Voraussetzung für die Annahme einer Meldung.

Wenn sich Ihre Meldung auf unsere **digitale Infrastruktur** bezieht (z. B. Website oder genutzte Services), kontaktieren Sie bitte: security@heidenhain.com

Hinweise für Sicherheitsforschende

HEIDENHAIN wird keine rechtlichen Schritte gegen meldende Personen einleiten, sofern die folgenden Bedingungen eingehalten werden:

- Keine Schädigung von Personen
- Tests nur im erforderlichen Umfang zur Bestätigung einer Schwachstelle
- Tests an Produktivsystemen nur mit ausdrücklicher Zustimmung
- Keine Beeinträchtigung der Verfügbarkeit (keine DoS-Angriffe), kein Social Engineering und kein Zugriff auf physische Infrastruktur
- Zugriff nur auf die zur Demonstration erforderlichen Daten; keine Änderung, Löschung oder Exfiltration von Daten
- Schutz der Sicherheit und Privatsphäre anderer
- Einhaltung geltender Gesetze
- Bereitschaft zur koordinierten Offenlegung (keine Veröffentlichung vor Ablauf eines einvernehmlich festgelegten Zeitraums)

Wir schätzen Ihre Hinweise sehr, die uns dabei helfen, Probleme schnell zu beheben.

Richtlinien für Sicherheitsforschende

- Informieren Sie uns so früh wie möglich über tatsächliche oder potenzielle Sicherheitsprobleme.
- Nutzen Sie Exploits nur im notwendigen Umfang zur Bestätigung der Schwachstelle.
- Geben Sie uns ausreichend Zeit zur Behebung. Wir veröffentlichen signifikante und bestätigte Schwachstellen auf CERT@VDE.
- Eine sofortige externe Veröffentlichung führt zu einer „Zero-Day"-Situation und setzt Systeme unserer Kunden – darunter kritische Infrastrukturen – unnötigen Risiken aus. Daher bitten wir ausdrücklich um koordinierte Offenlegung.

Meldung einer Schwachstelle

- Bitte nutzen Sie für die Übermittlung ausführlicher Schwachstellenberichte sowie zugehöriger Dateien und Nachweise unser Cyber-Security-Kontaktformular.
- **E-Mail:** product-security@heidenhain.com (Die angegebenen E-Mail-Adressen der security.txt dienen ausschließlich der ersten Kontaktaufnahme und sind nicht für die Übermittlung sensibler oder detaillierter Schwachstelleninformationen vorgesehen.)
- **Meldung über CERT@VDE:** https://www.certvde.com/de/service/schwachstelle-melden/

Inhalte der Meldung

Bitte geben Sie – wenn möglich – folgende Informationen an:

- Betroffenes Produkt oder Software (inkl. Identnummer und Firmware-/Versionsstand)
- Beschreibung der Schwachstelle, wo diese gefunden wurde und welche möglichen Auswirkungen zu erwarten sind
- Reproduzierbare Schritte (PoC, Skripte, Screenshots, Netzwerkdaten)
- Ob die Schwachstelle bereits öffentlich bekannt ist
- Zugehörige Dokumente (CVE, Mitteilungen, Release Notes)
- Idealerweise Beschreibung in englischer Sprache

Unser Bearbeitungsprozess

1. **Eingang:** Wir bestätigen den Eingang Ihrer Meldung.
2. **Analyse:** Wir untersuchen und reproduzieren die Schwachstelle und fordern bei Bedarf zusätzliche Informationen an.
3. **Handling:** Wir koordinieren die Behebung und halten Sie auf dem Laufenden.
4. **Offenlegung:** Sobald eine Lösung verfügbar oder veröffentlicht ist (je nachdem, was zuerst eintritt), veröffentlichen wir ein Security Advisory. CVE-Einträge werden gemeinsam mit CERT@VDE erstellt und nach CSAF veröffentlicht.

Inhalte unserer Security Advisories

Ein Security Advisory beinhaltet in der Regel:

- Beschreibung der Schwachstelle mit CVE-Referenz und CVSS-Score
- Betroffene Produkte und Versionen
- Informationen zu Workarounds und Maßnahmen zur Risikominderung
- Hinweise auf verfügbare Updates/Fixes

DR. JOHANNES HEIDENHAIN GmbH
Dr.-Johannes-Heidenhain-Straße 5
83301 Traunreut, Germany
☎ +49 8669 31-0
FAX +49 8669 32-5061
service@heidenhain.de

www.heidenhain.com

11/2026