Coordinated Vulnerability Disclosure (CVD) Policy

ZeroClamp · Zerobot® · Zerocob®

Status: July 2026 | Classification: Public | Version: 1.0

Scope: Digital products, components and publicly accessible web services of ZeroClamp (in particular ZeroClamp Zerobot and Zerocob)

1. Purpose & Scope

ZeroClamp takes the security of its products and publicly accessible web services seriously. This policy describes how security researchers, customers, partners and service technicians can responsibly report potential vulnerabilities to us and how we handle such reports.

This policy forms part of the ZeroClamp GmbH vulnerability handling process and is intended, in particular, to implement the requirements regarding coordinated vulnerability disclosure and the provision of a contact address pursuant to Annex I, Part II, points 5 and 6 of Regulation (EU) 2024/2847 ("Cyber Resilience Act").

This public policy describes the external reporting process. The internal handling, decision-making and reporting process is defined in the PSIRT Process Manual.

2. Our Commitment to Good-Faith Security Research (Safe Harbor)

If you comply with this policy, we will treat your report as good-faith security research, provided that your activities remain within the scope described herein and do not infringe the rights of third parties.

ZeroClamp will not initiate legal action solely as a result of a responsible vulnerability report, provided in particular that no data exfiltration, extortion, intentional disruption of operations or other violations of Sections 3 and 4 have occurred.

We will work with you to understand, assess and remediate the reported vulnerability as quickly as reasonably possible. Should a third party initiate legal action against you, we will state, where appropriate, that in our assessment you acted in good faith and within the framework of this policy.

3. What We Expect from You

- Report a suspected vulnerability as soon as possible after discovery.
- Allow us reasonable time to remediate the vulnerability before disclosing details publicly (see Section 8).
- Avoid privacy breaches, data exfiltration, persistent modifications and any disruption of system operations.
- Access only devices that you own or for which you have been explicitly authorized - never access production systems at customer sites without their consent.
- No physical attacks, social engineering, automated mass scanning, brute-force attacks or DoS/load testing against production systems.
- Treat all information obtained in the course of your research as confidential until coordinated disclosure has taken place.

> ***Safety notice:*** *Zerobot and Zerocob are machines incorporating moving robots, automated clamping devices and safety doors. Security testing* ***must never be performed on a system while it is in operation*** *- there is a real risk of physical injury.*

4. Scope

In Scope - ZeroClamp Digital Products and Web Services

Product/Component	Examples of Relevant Security Topics
Zerobot & Zerocob Control (Firmware + Web User Interface)	Authentication, access control, web vulnerabilities, integrity, logging
Wi-Fi Connectivity (Access Point, Wi-Fi Hub)	Encryption, default credentials, network segmentation
ZeroVise P100/P160 IoT (incl. wireless monitoring)	Wireless communication, manipulation of clamping data
Smart Operator	Wireless triggering, authentication
Machine Light Sensor	Parameter configuration, data integrity
Control/Data Interfaces (Ethernet, RS485, I/O)	Integrity, unauthorized control access
Publicly Accessible ZeroClamp Web Services	Vulnerabilities on zeroclamp.com, publicly accessible portals and online services operated by ZeroClamp

Out of Scope

- Purely mechanical products without digital elements (grippers, racks, zero-point clamping systems, vises)
- The operator's machine tool / CNC control (not part of the ZeroClamp product)
- The Nachi robot itself - please report vulnerabilities directly to NACHI EUROPE GmbH; for integration-related issues, we will coordinate as appropriate
- Vulnerabilities resulting exclusively from misconfiguration by the operator and not facilitated by insecure default settings, unclear documentation or missing product safeguards
- Volumetric DoS attacks, spam, social engineering, physical attacks
- Theoretical findings without a realistic attack path

If in doubt, please report the issue anyway - we will assess the scope together.

5. Reporting Channel

Channel	Details
E-Mail	security@zeroclamp.com
PGP Key	https://www.zeroclamp.com/security/pgp-key.txt
security.txt	https://www.zeroclamp.com/.well-known/security.txt
Language	German or English

For confidential information (PoC, exploit details, logs), please use PGP encryption. You will receive an automatic acknowledgement of receipt including a case number.

6. A Good Vulnerability Report Includes

- Affected product and version (e.g. Zerobot Firmware 12.11.3)
- Type of vulnerability and affected component/interface
- Step-by-step reproduction instructions (Proof of Concept, where possible)
- Potential impact (technical and, where identifiable, safety-related)
- Information about active exploitation, if applicable
- Your contact details for follow-up questions and whether you would like to be credited (Section 9)

The more complete the report, the faster we can assess and remediate the vulnerability.

7. Our Process & Response Times

Step	Target
Automatic technical acknowledgement of receipt with case number	Usually immediately
Personal acknowledgement by the Security Team	Within 2 business days
Initial assessment / triage	Within 5 business days
Status update	Regularly, at least every 14 days until remediation
Remediation	Depending on severity and ability to update (see Section 8)

> ***Escalation in urgent situations:*** *Reports indicating* ***active exploitation,*** *an* ***imminent threat*** *or potential* ***safety impact****, particularly involving robots or clamping devices, will be prioritized and immediately escalated through our internal escalation process. Please clearly identify such reports.*

Each valid report is opened internally as a PSIRT case and documented in an auditable manner.

8. Coordinated Disclosure

- We aim for coordinated disclosure: publication should take place only once a patch or effective workaround is available.
- Target timeframe: 90 days from acknowledgement of receipt. For complex remediation (e.g. on-site service for products already deployed in the field), this period may be extended by mutual agreement; in the event of active exploitation, it may be shortened.
- Upon request, we will credit you as the finder in the relevant Security Advisory and on our Security Researcher page.
- Please coordinate any public disclosure with us - where a CVE identifier is appropriate and available, we will coordinate its assignment or application.

Statutory reporting obligations remain unaffected by coordinated disclosure. Where the applicable legal requirements are met, ZeroClamp will report actively exploited vulnerabilities and severe incidents having an impact on the security of products with digital elements within the prescribed time limits via the reporting infrastructure provided for under the Cyber Resilience Act to the competent authorities.

9. Recognition

We recognize responsible security reports and, upon request, credit Security Researchers on our public Security Researcher page. We currently do not operate a monetary bug bounty program.

10. Confidentiality & Data Protection

- We treat your report and your identity as confidential.
- We process personal data exclusively for the purpose of handling the report in accordance with the GDPR.
- We will not disclose your identity to third parties without your consent, unless required by law.

11. Interface with Installed Base & Third-Party Components

- If a report concerns a third-party component integrated into the automation system (e.g. a Nachi robot or software libraries used by the product), we will assess our due diligence and vulnerability handling obligations under Article 13(5) and (6) of the CRA and, where necessary, forward the information to the relevant manufacturer or maintainer.

- If a report concerns devices already deployed in the field (Installed Base), we will coordinate information and update distribution with the affected operators.

12. Contact

ZeroClamp GmbH

Albert-Mayer-Straße 13, 83052 Bruckmühl, Germany

Security reports: security@zeroclamp.com

PGP & Policy: https://www.zeroclamp.com/security

Annex A - security.txt (Template according to RFC 9116)

```
Contact: mailto:security@zeroclamp.com
Encryption: https://zeroclamp.com/wp-content/uploads/2026/08/zeroclamp-public-key.asc
Policy: https://zeroclamp.com/wp-content/uploads/2026/08/security.txt
Preferred-Languages: de, en
Canonical: https://www.zeroclamp.com/.well-known/security.txt
Expires: 2028-07-30T00:00:00.000Z
```

Annex B - Version History

Version	Date	Change
1.0	July 2026	Initial version, derived from the ZeroClamp/Automation PSIRT Process Manual