Coordinated Vulnerability Disclosure (CVD) Policy

ZeroClamp · Zerobot® · Zerocob®

Stand: Juli 2026 | Klassifizierung: Öffentlich | Version: 1.0

Geltung: Digitale Produkte, Komponenten und öffentlich erreichbare Webangebote von ZeroClamp (insb. ZeroClamp Zerobot und Zerocob)

1. Zweck & Geltungsbereich

ZeroClamp nimmt die Sicherheit seiner Produkte und öffentlich erreichbaren Webangebote ernst. Diese Richtlinie beschreibt, wie Sicherheitsforscher, Kunden, Partner und Servicetechniker mögliche Schwachstellen verantwortungsvoll an uns melden können und wie wir damit umgehen.

Diese Richtlinie ist Bestandteil des Vulnerability-Handling-Prozesses der ZeroClamp GmbH und dient insbesondere der Umsetzung der Anforderungen an eine koordinierte Offenlegung von Schwachstellen und an die Bereitstellung einer Kontaktadresse gemäß Anhang I Teil II Nr. 5 und Nr. 6 der Verordnung (EU) 2024/2847 („Cyber Resilience Act“).

Diese öffentliche Policy beschreibt den Meldeweg nach außen. Der interne Bearbeitungs-, Entscheidungs- und Meldeprozess ist im PSIRT-Prozesshandbuch geregelt.

2. Unsere Zusage für gutgläubige Sicherheitsforschung (Safe Harbor)

Wenn Sie sich an diese Richtlinie halten, behandeln wir Ihre Meldung als gutgläubige Sicherheitsforschung, sofern sie im beschriebenen Geltungsbereich bleibt und keine Rechte Dritter verletzt.

ZeroClamp wird keine rechtlichen Schritte einleiten, die sich allein aus einer verantwortungsvollen Meldung ergeben, sofern insbesondere keine Datenexfiltration, Erpressung, absichtliche Betriebsbeeinträchtigung oder sonstigen Verstöße gegen die Abschnitte 3 und 4 vorliegen.

Wir arbeiten mit Ihnen zusammen, um die gemeldete Schwachstelle zügig zu verstehen, zu bewerten und zu beheben. Sollte ein Dritter rechtliche Schritte gegen Sie einleiten, werden wir darauf hinweisen, wenn Sie nach unserer Einschätzung in gutem Glauben und im Rahmen dieser Richtlinie gehandelt haben.

3. Was wir von Ihnen erwarten

- Melden Sie eine vermutete Schwachstelle so früh wie möglich nach Entdeckung.
- Geben Sie uns angemessene Zeit zur Behebung, bevor Sie Details veröffentlichen (siehe Abschnitt 8).
- Vermeiden Sie Datenschutzverletzungen, Datenexfiltration, dauerhafte Veränderungen und jede Beeinträchtigung des Anlagenbetriebs.
- Greifen Sie nur auf eigene oder ausdrücklich freigegebene Geräte zu — niemals auf produktive Kundenanlagen ohne deren Einwilligung.
- Keine physischen Angriffe, kein Social Engineering, keine automatisierten Massenscans, Brute-Force-Angriffe oder DoS/Lasttests gegen produktive Systeme.
- Behandeln Sie alle im Rahmen der Forschung erlangten Informationen vertraulich, bis eine koordinierte Offenlegung erfolgt ist.

> ***Sicherheitshinweis:*** *Der Zerocob ist eine Maschine mit beweglichem Roboter/Cobot, automatischen Spannmitteln und Schutztür. Sicherheitstests dürfen* ***niemals an einer in Betrieb befindlichen Anlage*** *durchgeführt werden — es besteht ein reales physisches Verletzungsrisiko.*

4. Geltungsbereich (Scope)

In-Scope — digitale ZeroClamp-Produkte und Webangebote

Produkt/Komponente	Beispiele für relevante Themen
Zerobot & Zerocob Steuerung (Firmware + Web-Bedienoberfläche)	Authentisierung, Zugriffskontrolle, Web-Schwachstellen, Integrität, Logging
WLAN-Anbindung (Access Point, WLAN-Hub)	Verschlüsselung, Default-Credentials, Netztrennung
ZeroVise P100/P160 IoT (inkl. drahtlose Überwachung)	Funkkommunikation, Manipulation der Spanndaten
Smart Operator	Funkgesteuerte Auslösung, Authentisierung
Sensor Maschinenleuchte	Parametrierung, Datenintegrität
Steuer-/Datenschnittstellen (Ethernet, RS485, I/O)	Integrität, unbefugter Steuerzugriff
Öffentlich erreichbare ZeroClamp-Webangebote	Schwachstellen auf zeroclamp.com, öffentlich erreichbare Portale und von ZeroClamp betriebene Onlinedienste

Out-of-Scope

- Rein mechanische Produkte ohne digitale Elemente (Greifer, Racks, Nullpunktspannsysteme, Schraubstöcke)
- Die Werkzeugmaschine / CNC-Steuerung des Betreibers (nicht Bestandteil des ZeroClamp-Produkts)
- Der Nachi Roboter selbst — bitte direkt an NACHI EUROPE GmbH melden; bei integrationsbedingten Problemen koordinieren wir uns
- Schwachstellen, die ausschließlich aus Fehlkonfiguration durch den Betreiber resultieren und nicht durch unsichere Standardeinstellungen, unklare Dokumentation oder fehlende Schutzmechanismen des Produkts begünstigt werden
- Volumetrische DoS-Angriffe, Spam, Social Engineering, physische Angriffe
- Theoretische Befunde ohne realistischen Angriffspfad

Im Zweifel: bitte trotzdem melden — wir bewerten den Scope gemeinsam.

5. Meldekanal

Kanal	Angabe
E-Mail	security@zeroclamp.com
PGP-Schlüssel	https://www.zeroclamp.com/security/pgp-key.txt
security.txt	https://www.zeroclamp.com/.well-known/security.txt
Sprache	Deutsch oder Englisch

Für vertrauliche Inhalte (PoC, Exploit-Details, Logs) bitten wir um PGP-Verschlüsselung. Sie erhalten eine automatische Eingangsbestätigung mit einer Fallnummer.

6. Eine gute Schwachstellenmeldung enthält

- Betroffenes Produkt und Version (z. B. Zerobot Firmware 12.11.3)
- Art der Schwachstelle und betroffene Komponente/Schnittstelle
- Schritt-für-Schritt-Reproduktion (Proof of Concept, sofern möglich)
- Mögliche Auswirkung (technisch und, falls erkennbar, sicherheitsbezogen/Safety)
- Hinweise auf aktive Ausnutzung, falls vorhanden
- Ihre Kontaktdaten für Rückfragen und ob Sie eine Nennung wünschen (Abschnitt 9)

Je vollständiger die Meldung, desto schneller können wir bewerten und beheben.

7. Unser Prozess & Reaktionszeiten

Schritt	Ziel
Automatische technische Eingangsbestätigung mit Fallnummer	In der Regel unmittelbar
Persönliche Bestätigung durch das Security-Team	Innerhalb von 2 Werktagen
Erste Bewertung / Triage	innerhalb von 5 Werktagen
Statusrückmeldung	regelmäßig, mindestens alle 14 Tage bis zur Behebung
Behebung	abhängig von Schweregrad und Updatefähigkeit (siehe Abschnitt 8)

> ***Eskalation bei akuter Lage:*** *Meldungen mit Hinweisen auf eine* ***aktive Ausnutzung,*** *eine unmittelbar* ***drohende Gefährdung*** *oder mögliche* ***Safety-Auswirkungen****, insbesondere durch Roboter oder Spannmittel, werden priorisiert und unverzüglich in den internen Eskalationsprozess überführt. Bitte kennzeichnen Sie solche Meldungen deutlich.*

Jede gültige Meldung wird intern als PSIRT-Case eröffnet und revisionsfest dokumentiert.

8. Koordinierte Offenlegung

- Wir streben eine koordinierte Offenlegung an: Veröffentlichung erst, wenn ein Patch oder wirksamer Workaround verfügbar ist.
- Richtwert: 90 Tage ab Eingangsbestätigung. Bei komplexer Behebung (z. B. Vor-Ort-Service an Bestandsanlagen) kann dieser Zeitraum in Abstimmung verlängert werden; bei aktiver Ausnutzung verkürzt.
- Wir nennen Sie auf Wunsch als Finder im Security Advisory (ZeroClamp Security Advisory, ZSA-Schema).
- Bitte stimmen Sie eine Veröffentlichung mit uns ab — Soweit eine CVE-Kennung angemessen und verfügbar ist, koordinieren wir deren Beantragung oder Zuordnung.

Gesetzliche Meldepflichten bleiben von der koordinierten Offenlegung unberührt. Sofern die gesetzlichen Voraussetzungen vorliegen, meldet ZeroClamp aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle innerhalb der vorgeschriebenen Fristen über die nach dem Cyber Resilience Act vorgesehene Meldeinfrastruktur an die zuständigen Stellen.

9. Anerkennung

Wir würdigen verantwortungsvolle Meldungen. Auf Wunsch nennen wir Finder in unseren Security Advisories und in einer öffentlichen Danksagung. Ein monetäres Bug-Bounty-Programm besteht derzeit nicht; dies kann sich künftig ändern.

10. Vertraulichkeit & Datenschutz

- Wir behandeln Ihre Meldung und Ihre Identität vertraulich.
- Personenbezogene Daten verarbeiten wir ausschließlich zur Bearbeitung der Meldung gemäß DSGVO.
- Wir geben Ihre Identität nicht ohne Ihre Zustimmung an Dritte weiter, soweit keine gesetzliche Pflicht entgegensteht.

11. Schnittstelle zu Bestand & Drittkomponenten

- Betrifft eine Meldung eine in der Automation integrierten Drittkomponente (z. B. Nachi-Roboter, eingesetzte Software-Bibliotheken), prüfen wir unsere Sorgfalts- und Behandlungspflichten nach CRA Art. 13 Abs. 5/6 und leiten die Information bei Bedarf an den jeweiligen Hersteller/Maintainer weiter.
- Betrifft eine Meldung Geräte im Feld (Installed Base), koordinieren wir Information und Update-Verteilung mit den betroffenen Betreibern.

12. Kontakt

ZeroClamp GmbH

Albert-Mayer-Straße 13, 83052 Bruckmühl, Deutschland

Sicherheitsmeldungen: security@zeroclamp.com

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

Anhang A — security.txt (Vorlage nach RFC 9116)

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

Anhang B — Versionshistorie

Version	Datum	Änderung
1.0	Juli 2026	Erstfassung, abgeleitet aus PSIRT-Prozesshandbuch ZeroClamp/Automation