OCTO Actuators GmbH
de Werth Straße 1
DE - 97947 Grünsfeld

Phone: +49 (0) 93 46 / 92 76 - 0
Fax: +49 (0) 93 46 / 92 76 - 399
www.octo-actuators.de

Cyber Resilience Act (CRA)

- CVD Richtlinie zur koordinierten Offenlegung von Schwachstellen -
- CVD Guideline on the Coordinated Disclosure of Vulnerabilities -

1. Zweck und Grundsatz / Purpose and principles

OCTO Actuators begrüßt verantwortungsvolle Meldungen von Schwachstellen in unseren Produkten mit digitalen Elementen. Ziel dieser Richtlinie ist, Meldungen sicher entgegenzunehmen, zu prüfen, zu beheben und – soweit vertretbar – koordiniert offenzulegen. Die Richtlinie gilt unabhängig davon, ob die meldende Person Kunde, Partner, Mitarbeiter oder externe Sicherheitsforscherin bzw. externer Sicherheitsforscher ist.

OCTO Actuators welcomes responsible reports of vulnerabilities in our products with digital elements. This policy explains how we securely receive, assess, remediate and, where appropriate, coordinate disclosure of reports. It applies whether the reporter is a customer, partner, employee or external security researcher.

2. Geltungsbereich / Scope

Diese Richtlinie gilt für von OCTO Actuators entwickelte oder vertriebene Produkte mit digitalen Elementen, insbesondere Möbelantriebe und zugehörige Steuerungssysteme innerhalb des jeweils definierten Sicherheits-Supportzeitraums: kabelgebundene Steuerungen und Schnittstellen, Funk- und BLE-Komponenten, Firmware, Embedded Software, Konfigurations- und Diagnosewerkzeuge, mobile Anwendungen sowie von OCTO Actuators betriebene Webportale, APIs und Cloud-Dienste, soweit vorhanden.

Nicht umfasst sind: Gebäude- und Personenschutz, Social Engineering gegen Mitarbeitende, Tests gegen fremde Systeme, DoS/DDoS- oder Resource-Exhaustion-Tests, Spam sowie physische Beschädigung. Systeme Dritter dürfen nur gemeldet, nicht getestet werden; wir leiten Meldungen nach Möglichkeit an den zuständigen Anbieter weiter.

This policy covers products with digital elements developed or distributed by OCTO Actuators, including furniture actuators and related control systems within the defined security support period: wired controllers and interfaces, radio and BLE components, firmware, embedded software, configuration and diagnostic tools, mobile applications, and OCTO Actuators-operated portals, APIs and cloud services where applicable.

Excluded are physical and personal security, social engineering against employees, testing third-party systems, DoS/DDoS or resource-exhaustion tests, spam and physical damage. Third-party systems may be reported but must not be tested; where possible, we will forward reports to the responsible provider.

3. Meldewege und Mindestangaben / Reporting channels and minimum information

Bevorzugter Meldeweg: Nutzen Sie das Sicherheits-Meldeportal auf der Website von OCTO Actuators: https://octo-actuators.de/cra. Alternativ können Meldungen an security@octo-actuators.de gesendet werden. Bitte keine vertraulichen Kundendaten oder Zugangsdaten unverschlüsselt übermitteln.

Eine Meldung sollte, soweit bekannt, enthalten: betroffene Produkt- und Versionsangaben, Testumgebung, reproduzierbare Schritte, Proof of Concept mit minimal notwendigem Detail, Auswirkungen, vermutete Schwere, Zeitpunkte und Kontaktdaten für Rückfragen. Anonyme Meldungen werden bearbeitet, soweit eine Prüfung möglich ist.

Preferred channel: use the OCTO Actuators security reporting portal: https://octo-actuators.de/cra. Alternatively, reports may be sent to security@octo-actuators.de. Do not send confidential customer data or credentials unencrypted.

Where known, include affected product and version, test environment, reproducible steps, a minimally detailed proof of concept, impact, estimated severity, dates and contact details. Anonymous reports will be handled where investigation is possible.

4. Regeln für Tests/Verhaltenskodex / Testing rules/code of conduct

- Testen Sie nur eigene Geräte, Konten und Daten oder holen Sie vorher eine ausdrückliche Genehmigung ein.
  Test only your own devices, accounts and data, or obtain explicit permission beforehand.
- Vermeiden Sie Zugriff auf fremde Daten, Datenänderung, Datenlöschung, dauerhafte Beeinträchtigung und Produktionsausfälle.
  Avoid accessing third-party data, changing or deleting data, persistent impairment and service outages.
- Beenden Sie Tests, sobald die Schwachstelle bestätigt ist; beschränken Sie Proofs of Concept auf das notwendige Maß.
  Stop testing once the issue is demonstrated; keep proofs of concept to the necessary minimum.
- Keine DoS/DDoS-, Spam-, Social-Engineering-, Massen-Scan- oder Resource-Exhaustion-Tests.
  No DoS/DDoS, spam, social-engineering, mass-scanning or resource-exhaustion tests.
- Behandeln Sie Informationen vertraulich und stimmen Sie eine Veröffentlichung mit uns ab.
  Treat information confidentially and coordinate any disclosure with us.

5. Rechtsschutz/Safe Harbor / Legal/safe harbor

OCTO Actuators beabsichtigt, gegen Personen, die nach dieser Richtlinie in gutem Glauben und innerhalb des beschriebenen Umfangs Sicherheitsforschung betreiben, keine rechtlichen Schritte einzuleiten, sofern sie keine Daten oder Systeme schädigen, keine Rechte Dritter verletzen und vertraulich handeln. Diese Zusage gilt nur im gesetzlich zulässigen Umfang, begründet keinen Verzicht auf Rechte und gilt nicht für böswilliges, betrügerisches oder gefährliches Verhalten. Bei Tests in Systemen Dritter kann OCTO Actuators keine Zusage abgeben.

OCTO Actuators intends not to pursue legal action against persons conducting security research in good faith and within this policy, provided they do not damage systems or data, violate third-party rights or disclose information irresponsibly. This commitment applies only to the extent permitted by law, does not waive any rights and does not cover malicious, fraudulent or dangerous conduct. OCTO Actuators cannot make commitments for third-party systems.

6. Bearbeitungsprozess und Zielzeiten / Handling process and target timelines

Phase / Phase	**Ziel** / Target	**Verantwortung** / Owner
Eingang bestätigen Acknowledge	2 Werktage; möglichst 48 Stunden 2 business days; target 48 hours	CVD-Kontakt
Triage und Bestätigung Triage and validation	10 Werktage 10 business days	Security + Engineering
Schweregrad Severity	Nach Validierung, anhand CVSS v4 als Hilfsmittel after validation, CVSS v4 as aid	Security
Status Updates	Alle 14 Tage bei offenem Fall every 14 days while open	Case owner
Mitigation Mitigation	Unverzüglich bei aktivem Angriff oder hohem Risiko immediately for active exploitation or high risk	Security + Management
Fix Fix	Ziel: 30/60/90 Tage nach Schwere; begründete Abweichungen kommunizieren target 30/60/90 days by severity; communicate justified deviations	Engineering + Product

Die angegebenen Zielzeiten stellen unverbindliche Zielgrößen im Rahmen unseres Bearbeitungsprozesses dar und begründen keine automatische gesetzliche Patch-Frist. Gesetzliche Melde- und Informationspflichten im Rahmen des Cyber Resilience Acts (CRA) bleiben hiervon unberührt.

These timelines represent internal target goals within our handling process and do not constitute a statutory patch deadline. Statutory notification and reporting obligations under the Cyber Resilience Act (CRA) remain unaffected.

7. Koordinierte Veröffentlichung / Coordinated disclosure

Wir veröffentlichen Informationen zu behobenen Schwachstellen grundsätzlich erst, wenn eine Abhilfe verfügbar ist und Kunden eine angemessene Möglichkeit zur Aktualisierung hatten. Wir stimmen Inhalt und Zeitpunkt nach Möglichkeit mit der meldenden Person ab. Als Richtwert schlagen wir 30 Tage nach Veröffentlichung der Abhilfe vor; bei aktiver Ausnutzung, hoher Gefahr oder fehlender Abstimmung kann OCTO Actuators früher oder später veröffentlichen. Bei begründeten Sicherheitsrisiken kann die Veröffentlichung verzögert werden. Security Advisories enthalten mindestens betroffene Produkte/Versionen, Schweregrad, Auswirkungen, Abhilfe und Update-Hinweise.

We generally publish information about fixed vulnerabilities only after a remedy is available and customers have had a reasonable opportunity to update. Where possible, we coordinate content and timing with the reporter. As a guideline, we propose disclosure 30 days after the remedy is published; in cases of active exploitation, high risk or no response, OCTO Actuators may disclose earlier or later. Publication may be delayed where justified security risks outweigh the benefits. Advisories include affected products/versions, severity, impact, remedy and update guidance.

8. Anerkennung, CVE und keine Prämien / Recognition, CVE and no rewards

OCTO Actuators zahlt keine Prämien und betreibt kein Bug-Bounty-Programm. Eine namentliche Anerkennung oder die Nennung eines Alias erfolgt nur auf ausdrücklichen Wunsch. Eine CVE-ID oder sonstige Registrierung kann je nach Zuständigkeit und Sinnhaftigkeit beantragt bzw. koordiniert werden; sie wird nicht für jeden Fall garantiert.

OCTO Actuators does not pay rewards and does not operate a bug-bounty programme. A name or alias will be credited only with the reporter's explicit consent. A CVE ID or other registration may be requested or coordinated where appropriate and within the relevant authority's scope; it is not guaranteed for every case.

9. Datenschutz, Vertraulichkeit und Aufbewahrung / Privacy, confidentiality and retention

Wir verarbeiten Kontaktdaten und die in einer Meldung enthaltenen Informationen zur Bearbeitung, Kommunikation, Sicherheitsverbesserung und Erfüllung gesetzlicher Pflichten. Bitte übermitteln Sie nur notwendige personenbezogene Daten. Zugriff erhalten nur Personen mit Aufgabenbedarf. Details werden so lange aufbewahrt, wie es für Bearbeitung, Nachweis, Produktsicherheit und gesetzliche Pflichten erforderlich ist; konkrete Fristen werden im internen Löschkonzept festgelegt.

We process contact details and report information to handle reports, communicate, improve security and comply with legal obligations. Please provide only necessary personal data. Access is limited to those who need it for their role. Details are retained only as long as needed for handling, evidence, product safety and legal obligations; specific periods are defined in the internal deletion schedule.

10. Änderungen und Kontakt / Changes and contact

Diese Richtlinie wird mindestens jährlich und zusätzlich bei wesentlichen Produkt-, Prozess- oder Rechtsänderungen überprüft. Version, Freigabedatum und verantwortliche Stelle werden dokumentiert. Kontakt: security@octo-actuators.de; bevorzugter Meldeweg: https://octo-actuators.de/cra.

This policy is reviewed at least annually and whenever there are material product, process or legal changes. Version, approval date and owner are documented. Contact: security@octo-actuators.de; preferred reporting channel: https://octo-actuators.de/cra.

Johannes Schneider
Geschäftsführung

Grünsfeld 13.08.2026