BOWE GROUP

BOWE.COM

COORDINATED VULNERABILITY DISCLOSURE POLICY

BOWE GROUP

Version: 1.2

Gültig ab: 11.09.2026

Klassifizierung: Öffentlich – zur Veröffentlichung auf bowe.com

BOWE GROUP
a brand of
BÖWE SYSTEC GmbH

INHALTSVERZEICHNIS

1. ZWECK

Die Sicherheit unserer Produkte, Dienstleistungen und Kunden hat für die BOWE GROUP höchste Priorität. Trotz sorgfältiger Entwicklung, Qualitätssicherung sowie technischer und organisatorischer Sicherheitsmaßnahmen lässt sich das Auftreten von Schwachstellen nicht vollständig ausschließen.

Diese Coordinated Vulnerability Disclosure Policy (im Folgenden „CVD-Policy" oder „Richtlinie") beschreibt, wie externe Sicherheitsforschende, Kunden und andere Parteien potenzielle Sicherheitslücken in Produkten, Anwendungen und Diensten der BOWE GROUP melden können und wie die BOWE GROUP mit solchen Meldungen umgeht.

Ziel dieser Richtlinie ist die verantwortungsvolle, koordinierte und nachvollziehbare Behandlung gemeldeter Schwachstellen, um Risiken für Kundinnen und Kunden, Systeme und die Allgemeinheit zu minimieren.

2. GELTUNGSBEREICH

2.1 IM GELTUNGSBEREICH

Diese Richtlinie gilt für alle Produkte mit digitalen Elementen, die von der BOWE GROUP hergestellt, in der EU in Verkehr gebracht oder betrieben werden.

2.2 NICHT IM GELTUNGSBEREICH

- Systeme, Anlagen oder sonstige Geräte, die nicht im Eigentum der an dieser Richtlinie beteiligten Parteien stehen.

Werden Schwachstellen in Systemen entdeckt oder vermutet, die nicht von dieser Richtlinie erfasst sind, bitten wir darum, diese direkt an den jeweiligen Hersteller, Betreiber oder die zuständige Behörde zu melden.

3. MELDUNG EINER SICHERHEITSLÜCKE

Sicherheitslücken können wie folgt gemeldet werden:

E-Mail: product-security@bowe.com

Um eine zügige Bearbeitung zu ermöglichen, muss die Meldung folgende Angaben enthalten:

- Betroffenes Produkt oder System
- Betroffener Kunde (Name, Auftragsnummer), sofern zutreffend
- Produktversion

- Beschreibung der Schwachstelle
- Angabe, ob eine aktive Ausnutzung der Schwachstelle bekannt ist
- Schritte zur Reproduktion
- Proof of Concept, sofern vorhanden
- Kontaktdaten für Rückfragen

Wir bitten darum, ausschließlich die für die Bewertung der Schwachstelle erforderlichen Informationen zu übermitteln und auf die Übersendung nicht notwendiger personenbezogener oder vertraulicher Daten Dritter zu verzichten.

Die Meldung kann in deutscher oder englischer Sprache erfolgen.

4. UNSERE VERPFLICHTUNGEN

Wenn Sie im Einklang mit dieser Richtlinie mit uns zusammenarbeiten, können Sie von uns erwarten, dass wir:

- den Eingang Ihrer Meldung grundsätzlich innerhalb von fünf Arbeitstagen bestätigen und gemeinsam mit Ihnen die gemeldete Schwachstelle nachvollziehen und validieren.
- Sie, soweit möglich und angemessen, über den Fortschritt der Bearbeitung informieren.
- erkannte Schwachstellen unter Berücksichtigung der betrieblichen und technischen Rahmenbedingungen zeitnah beheben oder geeignete risikomindernde Maßnahmen ergreifen.
- für Sicherheitsforschung, die im Einklang mit den Kapiteln 5 und 6 dieser Richtlinie erfolgt, den dort beschriebenen Safe-Harbor-Schutz gewähren.

5. ERWARTETES VERHALTEN VON SICHERHEITSFORSCHENDEN

Wir begrüßen Sicherheitsforschung in gutem Glauben („good-faith security research") und bitten um die Einhaltung der nachfolgenden Regeln. Die vollständige Einhaltung dieser Regeln ist Voraussetzung für den in Kapitel 6 beschriebenen Safe-Harbor-Schutz.

5.1 ERLAUBTE AKTIVITÄTEN

- Identifikation und Dokumentation von Sicherheitslücken
- Durchführung minimal notwendiger Tests zur Verifikation
- Meldung der Schwachstelle ausschließlich an die BOWE GROUP über den in Kapitel 3 genannten Meldeweg
- Vertrauliche Behandlung der Erkenntnisse
- Sicherheitsuntersuchungen in eigenen Testumgebungen oder in ausdrücklich autorisierten Umgebungen

5.2 NICHT ERLAUBTE AKTIVITÄTEN

- Zugriff auf Daten Dritter
- Veränderung oder Löschung von Daten
- Unterbrechung von Diensten
- Denial-of-Service-Angriffe
- Social Engineering gegen Mitarbeitende oder Kunden
- Installation von Schadsoftware
- Physische Manipulation von Kundenanlagen
- Tests an Produktivsystemen von Kunden ohne deren ausdrückliche Zustimmung
- Tests an laufenden Maschinen
- Manipulation von SPS-, CNC-, Roboter- oder Maschinensteuerungen
- Änderungen von Prozessparametern
- Umgehung von Sicherheits- oder Schutzfunktionen
- Aktivitäten, die Auswirkungen auf Arbeitssicherheit, Anlagensicherheit oder Produktqualität haben können
- Last- oder Stresstests auf produktiven OT-Systemen

5.3 VERHALTEN BEI UNBEABSICHTIGTEM DATENZUGRIFF

Wird bei Testaktivitäten unbeabsichtigt auf sensible oder personenbezogene Daten zugegriffen, sind sämtliche Aktivitäten unverzüglich einzustellen. Der Vorfall ist im Rahmen der Meldung zu dokumentieren; die betroffenen Daten dürfen darüber hinaus weder eingesehen, gespeichert, weiterverarbeitet noch weitergegeben werden.

6. SAFE HARBOR

Wir möchten Sicherheitsforschende, die sich in gutem Glauben und im Einklang mit dieser Richtlinie engagieren, nicht rechtlich belangen.

6.1 VORAUSSETZUNG

Der in diesem Kapitel beschriebene Safe-Harbor-Schutz gilt ausschließlich, wenn und soweit die meldende Person sämtliche in Kapitel 5 genannten Bedingungen vollständig und durchgehend einhält – insbesondere, dass sie:

- ausschließlich die in Kapitel 5.1 als erlaubt bezeichneten Aktivitäten durchführt,
- keine der in Kapitel 5.2 als nicht erlaubt bezeichneten Aktivitäten vornimmt,
- im Falle eines unbeabsichtigten Zugriffs auf sensible oder personenbezogene Daten wie in Kapitel 5.3 beschrieben unverzüglich handelt, und
- die Schwachstelle ausschließlich über den in Kapitel 3 genannten Meldeweg berichtet.

6.2 UMFANG DER ZUSAGE

Sofern die Voraussetzungen aus Kapitel 6.1 erfüllt sind, betrachten wir die im Rahmen der Meldung durchgeführte Sicherheitsforschung als von der BOWE GROUP autorisierte Tätigkeit. Wir werden gegen die meldende Person keine zivil- oder strafrechtlichen Schritte im Zusammenhang mit der Entdeckung, Untersuchung und Meldung der Schwachstelle einleiten und uns im Rahmen des uns Möglichen dafür einsetzen, dass auch Dritte hiervon absehen, soweit die betreffenden Aktivitäten im Namen und Auftrag der meldenden Person im Rahmen dieser Richtlinie erfolgten.

6.3 GRENZEN DER ZUSAGE

Diese Zusage:

- gilt ausschließlich für die konkret gemeldete Schwachstelle und die zu ihrer Verifikation notwendigen Aktivitäten;
- begründet keinen eigenen Anspruch gegenüber Dritten (z. B. betroffenen Kunden) und lässt deren eigene Rechte unberührt;
- gilt nicht für Handlungen, die unabhängig von dieser Richtlinie gegen geltendes Recht verstoßen;
- kann von der BOWE GROUP für künftige Meldungen jederzeit geändert werden; bereits regelkonform eingereichte Meldungen bleiben von einer späteren Änderung unberührt.

7. BEWERTUNG UND PRIORISIERUNG

Wir bemühen uns, eingehende Meldungen zeitnah zu bewerten und zu beantworten.

Jede gemeldete Schwachstelle wird insbesondere hinsichtlich folgender Kriterien bewertet:

- Ausnutzbarkeit
- Auswirkungen auf die Vertraulichkeit
- Auswirkungen auf die Integrität
- Auswirkungen auf die Verfügbarkeit
- Auswirkungen auf die funktionale Sicherheit

8. KOORDINIERTE OFFENLEGUNG

Wir bevorzugen eine koordinierte Offenlegung (Coordinated Vulnerability Disclosure). Der übliche Ablauf ist:

1. Eingang der Meldung
2. Analyse und Risikobewertung
3. Entwicklung einer Behebung oder Gegenmaßnahme
4. Bereitstellung eines Updates

5. Information betroffener Kunden
6. Bereitstellung eines Security Advisories

Wir bitten meldende Personen, von einer Veröffentlichung abzusehen, bis ein Fix bereitgestellt wurde oder gemeinsam eine andere Vorgehensweise vereinbart wurde.

In gesetzlich vorgesehenen Fällen (insbesondere bei aktiv ausgenutzten Schwachstellen oder schwerwiegenden Sicherheitsvorfällen) kann die BOWE GROUP zusätzlichen gesetzlichen Melde- und Berichtspflichten gegenüber den zuständigen Behörden unterliegen; dies bleibt von dieser Richtlinie unberührt.

9. UMGANG MIT MELDUNGEN

Wir schätzen verantwortungsvolle Meldungen sehr. Aktuell betreibt die BOWE GROUP kein Bug-Bounty-Programm und leistet keine finanziellen Vergütungen für Schwachstellenmeldungen.

10. DATENSCHUTZ

Personenbezogene Daten, die im Rahmen einer Schwachstellenmeldung übermittelt werden, werden ausschließlich zur Bearbeitung der Meldung verwendet.

Die Verarbeitung erfolgt gemäß den geltenden Datenschutzbestimmungen, insbesondere der Datenschutz-Grundverordnung (DSGVO).

Die Daten werden nur den an der Untersuchung beteiligten Personen zugänglich gemacht und nach Abschluss des Vorgangs gemäß unseren internen Aufbewahrungsrichtlinien gelöscht oder archiviert.

Weitere Informationen zur Verarbeitung personenbezogener Daten finden Sie in unserer Datenschutzerklärung unter Datenschutz.