Coordinated Vulnerability Disclosure (CVD) Policy
Richtlinie zur koordinierten Offenlegung von Schwachstellen

1. Zweck dieser Richtlinie
Die Bausch+Ströbel SE + Co. KG („Bausch+Ströbel“) verpflichtet sich zu einem verantwortungsvollen, koordinierten Umgang mit Sicherheitslücken in seinen Produkten und digitalen Services.
Diese CVD-Policy beschreibt, wie Schwachstellen gemeldet, behandelt, behoben und offengelegt werden.

Diese Richtlinie folgt den Anforderungen aus:
- Cyber Resilience Act (EU) 2024/2847
- BSI TR-03183 Teil 3 (Vulnerability Reports and Notifications)

2. Geltungsbereich
Diese Richtlinie gilt für Produkte mit digitalen Elementen (weiterführende genannt: Produkte) und digitale Services von Bausch+Ströbel
- Maschinen und Softwareprodukte von Bausch+Ströbel
- Digitale Services, Cloud- und Remote-Lösungen

Nicht abgedeckt sind:
- Sicherheitsprobleme in Systemen Dritter außerhalb des Einflussbereichs von Bausch+Ströbel
- Physische Angriffe ohne Cyber-Bezug

3. Meldung von Schwachstellen
Schwachstellen können gemeldet werden über:

E-Mail (bevorzugt, verschlüsselt): psirt@bausch-stroebel.com

Die Kontaktdaten sind unter folgender Unternehmenswebsite abrufbar:
https://www.bausch-stroebel.com/de/unternehmen/security-advisories-psirt

Weitere Kontaktdaten sind in der öffentlich zugänglichen security.txt abrufbar:
https://www.bausch-stroebel.com/.well-known/security.txt

4. Was gilt als gültige Schwachstelle?
Eine Schwachstelle gilt als gültig, wenn:
- sie eines unserer Produkte oder Services betrifft und
- sie die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Nichtabstreitbarkeit oder Zuverlässigkeit beeinträchtigen kann

Nicht als gültige Schwachstellen gelten z.B.:
- Ergebnisse automatisierter Scans ohne Kontext oder Nachweis
- Fehlkonfigurationen außerhalb unseres Verantwortungsbereichs

5. Erwartete Informationen
Um die Meldung effizient bearbeiten zu können, sind folgende Daten erforderlich:
- Produktname und betroffene Version
- Eine detaillierte Beschreibung der Schwachstelle
- Schritte zur Reproduktion (Proof-of-Concept)
- Mögliche Auswirkungen (z. B. Remote Code Execution)

6. Verhaltensregeln (Safe Harbor)

Wenn Sie sich an die folgenden Regeln halten, wird Bausch+Ströbel keine rechtlichen Schritte gegen Sie einleiten:

+ Nutzen Sie Schwachstellen nicht aus (z.B. kein Download vertraulicher Daten, keine Veränderung von Systemen)
+ Führen Sie keine Denial-of-Service-Angriffe (DoS) oder Social-Engineering-Tests gegen unsere Beschäftigten durch
+ Geben Sie Informationen zur Schwachstelle erst dann an Dritte weiter, wenn wir eine Lösung bereitgestellt haben (Coordinated Disclosure)
+ Handeln Sie stets in gutem Glauben und unter Einhaltung geltender Gesetze

7. Zusicherungen von Bausch+Ströbel

Bausch+Ströbel sichert Meldenden zu:

+ Vertrauliche Behandlung der Meldung (soweit rechtlich zulässig)
+ Keine rechtlichen Schritte bei Meldungen in gutem Glauben. Dies gilt nicht, wenn offensichtlich erkennbare kriminelle oder nachrichtendienstliche Absichten oder Handlungen vorliegen
+ Keine Verpflichtung zur Unterzeichnung eines NDA (Non-Disclosure Agreement, Vertraulichkeitsvereinbarung, Geheimhaltungsvereinbarung)
+ Empfehlung und Unterstützung für verschlüsselte Kommunikation
+ Einen festen Ansprechpartner während des gesamten CVD-Prozesses
+ Die Schwachstelle so schnell wie möglich zu schließen

8. Ablauf des CVD-Prozesses

1) Eingang und Registrierung der Meldung
2) Validierung der Schwachstelle
3) Risikobewertung, z.B. CVSS (Common Vulnerability Scoring System, Einheitliches System zur Bewertung von Schwachstellen), Exploitierbarkeit (Ausnutzbarkeit)
4) Remediation (Behebung) oder Mitigation (Maßnahmen, die das Risiko oder die Auswirkungen einer Bedrohung verringern)
5) Information der betroffenen Nutzer
6) Koordinierte Offenlegung

Bei aktiv ausgenutzten Schwachstellen erfolgt eine enge Abstimmung mit dem zuständigen nationalen CSIRT (In Deutschland CERT BUND, BSI).

9. Reaktionszeiten

Bausch+Ströbel verpflichtet sich zu folgenden Reaktionszeiten:
≤ 5 Arbeitstage: erste qualifizierte Rückmeldung
≤ 10 Arbeitstage: technische Einschätzung oder Status-Update
Diese Rückmeldungen erfolgen nicht automatisiert

10. Offenlegung & Information

+ Behebbare Schwachstellen werden über Sicherheitsupdates adressiert
+ Betroffene Nutzer werden unverzüglich informiert
+ Sicherheitsinformationen werden als Security Advisories (Sicherheitswarnung) bereitgestellt
+ Veröffentlichung erfolgt bevorzugt maschinenlesbar, in einem internationalen, maschinenlesbaren Standard für Sicherheitswarnungen (CSAF, Common Security Advisory Framework)

Die öffentliche Offenlegung erfolgt in der Regel innerhalb von 90 Tagen, sofern keine sicherheitsrelevanten Gründe dagegensprechen

11. Ende des CVD-Prozesses

Ein CVD-Vorgang gilt als abgeschlossen, wenn:

+ ein Patch oder eine Mitigation veröffentlicht wurde und
+ betroffene Nutzer informiert wurden oder
+ sich die Meldung als unbegründet herausstellt.

12. Kontakt & Aktualisierung

Das Product Security Incident Response Team (PSIRT) ist erreichbar unter:
E-Mail (bevorzugt, verschlüsselt): psirt@bausch-stroebel.com

Diese Richtlinie wird mindestens jährlich überprüft und bei Bedarf aktualisiert.