e.battery systems AG
Mähdlegasse 1a
6850 Dornbirn, Austria

Richtlinie zur koordinierten Offenlegung von Sicherheitslücken

Coordinated Vulnerability Disclosure – CVD

Inhaltsverzeichnis

1. Geltungsbereich 2
2. Meldung einer Sicherheitslücke 2
3. Unser Umgang mit Meldungen 2
4. Erwartungen an Hinweisgeber 3
5. Good-Faith-Regelung 3
6. Nicht vom Geltungsbereich umfasst 3
7. Koordinierte Offenlegung 3
8. Kontakt 3

Unser Engagement für Sicherheit

Die Sicherheit unserer Produkte, Softwarelösungen, Dienstleistungen und IT-Systeme hat für uns höchste Priorität. Wir begrüßen Hinweise von Sicherheitsforschern, Kunden, Partnern und anderen Dritten, die dazu beitragen, potenzielle Sicherheitslücken frühzeitig zu erkennen und zu beheben.
Diese Richtlinie beschreibt den Prozess zur verantwortungsvollen Meldung von Sicherheitslücken und die Zusammenarbeit zwischen Hinweisgebern und unserem Unternehmen.

1. Geltungsbereich

Diese Richtlinie gilt für Sicherheitslücken in allen Produkten der ebs group einschließlich Batteriesystemen, Batterie-Management-Systemen, Firmware, Softwareanwendungen, Kundenportalen, Websites und zugehöriger IT-Infrastruktur, die von unserem Unternehmen betrieben wird.

2. Meldung einer Sicherheitslücke

Wenn Sie eine Sicherheitslücke entdeckt haben, bitten wir Sie, uns diese verantwortungsvoll mitzuteilen.

Bitte senden Sie Ihre Meldung an:
security@ebs-group.io

Bitte geben Sie nach Möglichkeit folgende Informationen an:

- Beschreibung der Schwachstelle
- Betroffenes Produkt, System oder Dienst
- Schritte zur Reproduzierbarkeit
- Mögliche Auswirkungen der Schwachstelle
- Screenshots, Logdateien oder Proof-of-Concept
- Ihre Kontaktdaten für Rückfragen

3. Unser Umgang mit Meldungen

Bei einer Meldung werden wir:

- den Eingang der Meldung zeitnah bestätigen,
- die gemeldete Schwachstelle prüfen,
- das Risiko und die Auswirkungen bewerten,
- erforderliche Maßnahmen zur Behebung einleiten,
- den Melder über den Fortschritt informieren, soweit angemessen,
- eine koordinierte Veröffentlichung der Schwachstelle anstreben.

4. Erwartungen an Hinweisgeber

Wir bitten alle Hinweisgeber:

- keine Daten von Kunden, Mitarbeitern oder Dritten einzusehen, zu verändern oder zu löschen,
- nur die zur Verifikation erforderlichen Tests durchzuführen,
- keine Systeme unnötig zu beeinträchtigen,
- keine Denial-of-Service-Angriffe durchzuführen,
- keine Schadsoftware einzusetzen,
- gefundene Schwachstellen bis zur Behebung vertraulich zu behandeln.

5. Good-Faith-Regelung

Personen, die Schwachstellen nach dieser Richtlinie in guter Absicht melden und diese Richtlinie einhalten, müssen keine rechtlichen Schritte durch unser Unternehmen befürchten.

6. Nicht vom Geltungsbereich umfasst

Folgende Aktivitäten sind ausdrücklich nicht von dieser Richtlinie abgedeckt:

- Social-Engineering-Angriffe
- Phishing-Kampagnen
- Physische Angriffe auf Gebäude oder Einrichtungen
- Denial-of-Service-Tests (DoS/DDoS)
- Spam-Kampagnen
- Angriffe auf Systeme von Kunden oder Drittanbietern
- Aktivitäten, die zu Datenschutzverletzungen oder Betriebsunterbrechungen führen

7. Koordinierte Offenlegung

Wir unterstützen die koordinierte Offenlegung von Sicherheitslücken. Wir bitten darum, gefundene Schwachstellen nicht öffentlich bekannt zu machen, bevor ausreichend Zeit für die Analyse und Behebung der Schwachstelle eingeräumt wurde oder eine gemeinsame Abstimmung erfolgt ist.
Sobald eine Behebung verfügbar ist, veröffentlichen wir bestätigte Schwachstellen als Security Advisory unter https://ebs-group.io/group#cybersecurity. Dort nennen wir das betroffene Produkt und die Version, den Schweregrad, das verfügbare Update und gegebenenfalls einen Workaround.

8. Kontakt

Für Meldungen von Sicherheitslücken und sicherheitsrelevante Anfragen:
security@ebs-group.io