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

Coordinated Vulnerability Disclosure Policy

Contents

1. Scope 2
2. Reporting a Vulnerability 2
3. Our Commitment 2
4. Expectations for Researchers 2
5. Safe Harbor 3
6. Out of Scope 3
7. Coordinated Disclosure 3
8. Contact 3

Our Commitment to Security

The security of our products, software solutions, services, and IT systems is of utmost importance to us. We welcome reports from security researchers, customers, partners, and other third parties that help us identify and address potential vulnerabilities.
This policy describes the process for responsible vulnerability reporting and cooperation between reporters and our organization.

1. Scope

This policy applies to vulnerabilities affecting all ebs group products, including battery systems, battery management systems, firmware, software applications, customer portals, websites and IT services that are operated by our company.

2. Reporting a Vulnerability

If you believe you have discovered a security vulnerability, please report it responsibly.

Please submit your report to:
security@ebs-group.io

When possible, please include:

- A detailed description of the vulnerability
- The affected product, system, or service
- Steps required to reproduce the issue
- Potential impact of the vulnerability
- Screenshots, log files, or proof-of-concept information
- Your contact details for follow-up questions

3. Our Commitment

When a vulnerability is reported in good faith, we will:

- Acknowledge receipt of the report promptly
- Investigate the reported vulnerability
- Assess the potential risks and impacts
- Take appropriate remediation measures
- Keep the reporter informed of significant progress where appropriate
- Strive for coordinated disclosure of confirmed vulnerabilities

4. Expectations for Researchers

We ask security researchers to:

- Avoid accessing, modifying, or deleting data belonging to customers, employees, or third parties
- Conduct only the testing necessary to verify the vulnerability

- Avoid unnecessary disruption of systems or services
- Refrain from denial-of-service testing
- Not deploy malware or malicious code
- Keep discovered vulnerabilities confidential until remediation has been completed

5. Safe Harbor

Provided that you act in good faith and comply with this policy, we will not initiate legal action against you for your security research activities or vulnerability report.

6. Out of Scope

The following activities are not covered by this policy:

- Social engineering attacks
- Phishing campaigns
- Physical attacks against facilities or personnel
- Denial-of-Service (DoS/DDoS) testing
- Spam campaigns
- Attacks against customer or third-party systems
- Activities that result in privacy violations or service disruption

7. Coordinated Disclosure

We support the coordinated disclosure of vulnerabilities. We ask researchers not to publicly disclose a vulnerability until sufficient time has been provided for investigation and remediation, or until mutual agreement has been reached.
Once a fix is available, we publish confirmed vulnerabilities as a security advisory at https://ebs-group.io/en/the-company#cybersecurity. Each advisory lists the affected product and version, the severity, the available update and, where applicable, a workaround.

8. Contact

For vulnerability reports and security-related inquiries:
security@ebs-group.io