Coordinated Vulnerability Disclosure Policy

(CVD Policy)

Effective Date: 2026-09-11
Last Updated: 2026-08-28
Version: 1.0
Document Owner: Product Security Incident Response Team (PSIRT)
Classification: Public

This policy is published in accordance with prEN 40000-1-3 (PRE-2) and ISO/IEC 29147.

1. Introduction and Commitment

At Inventus Power, Inc, we attach great importance to the security of our products and users. We are committed to providing secure products, including but not limited to our battery chargers, rechargeable battery packs, battery management systems, Internet of Things (IoT) devices, and related firmware/software.

We recognize that security vulnerabilities may be discovered during the lifecycle of a product (including its software and hardware components). To this end, we have established this Coordinated Vulnerability Disclosure Policy. We welcome and appreciate security researchers, industry partners, and users reporting potential security vulnerabilities to us in a responsible manner.

2. Scope

Within scope: We encourage responsible reporting of vulnerabilities affecting the following products:

- Hardware products: All products subject to the EU Cyber Resilience Act (CRA), including but not limited to battery chargers, rechargeable battery packs, related control units, Internet of Things (IoT) devices.
- Embedded software/firmware: All embedded software/firmware subject to the CRA, including but not limited to MCU firmware, bootloaders, and communication protocol stacks.

Out of scope: The following are generally not within the scope of this policy:

- Denial of Service (DoS/DDoS) attacks.
- Social engineering attacks against our employees or customers (phishing, vishing, etc.).
- Physical attacks or tampering with devices.
- Issues that require physical access to the device and cannot be exploited remotely.

3. Vulnerability Reporting Guidelines

We provide the following methods for receiving vulnerability reports:

1. Dedicated vulnerability reporting email: PSIRT@inventuspower.com. Vulnerability information is extremely sensitive; we strongly recommend that all emails containing security vulnerability reports sent to us be encrypted using PGP/GPG keys.

   Key fingerprint: 28681B11B390E352367546BFCD7703A0AE37F2CB

   PGP/GPG key:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGqRVCsBDADHwqpYb3UAN0dAt46/d70VP2r9t1ITb613vcCxkkPVNoscI8Ff
cQjin0tTafZyfQ5kPWxIJXn5+351kblDAcTwKqr7mpq2M6IH/cKVLbTueFJ9Mge5
```

```
5Vih75hxI+KiUZ5TozN/oE2AnoLATLPlJqofPZbJi3kB8d4Gjg2jBEuRe7IVckl+
rvhwgxZkhe0UyYSuBIj84y1jup50Yn7WktoVdSaFt7nSb6K63WjN4AS2CR0nEGjt
9pIAHi/Qe9xYVX0/xVKwSh87udbQHc0oJM+vC4qnBcrmM6bvKBP1HmpzHU5u71DI
Km+KpIZdZJ/M+jRvSvbMcIJJQtTtpp6RwD5K+w89H1+Bu+aP2seqL+roP/4WrLCO
v46jUM3YckKP9usBMUbzPBOZFGUjC4sjEwM3d79omOkO9V4Qc8O2jHxQmWVq4l96
DGkEdfwUOrRySwoO+bEoePLK22dIZvMILSUW8HSNQui7EIXcu39sy6niHfq7DBWL
8um7krQXuVgeUYUAEQEAAbQjQ2FyZXkgTGl1IDxQU0lSVEBpbnZlbnR1c3Bvd2Vy
LmNvbT6JAfMEEwEIAF0WIQQoaBsRs5DjUjZ1Rr/NdwOgrjfyywUCapFUKxsUgAAA
AAAEAA5tYW51MiwyLjUrMS4xMiwyLDECGwMFCQPEPwUFCwkIBwICIgIGFQoJCAsC
BBYCAwECHgcCF4AACgkQzXcDoK438stqKwv/dXhKQeLC4b3sWFkYhqt2EdTWLwG7
qjInsWboAnHtKilvgbSkM5Mj/6XMn7fMJ1qyfSJ/FwsEA36OJzFna2Om0ut7u4oQ
R5+gZaVJ+ph1Oj4IpwkCFkYmcq/7UkqU3v8gJf4vT54RTDFz5i9s6hOCTKZSjo9p
HIa/hxdtNcnsIZJY03Fnd5oQotVkJKxYUglPlNhCfLSESJzYnhe3do7bly0olUzp
F88WJCmrSxXBO/kptd15klHaojJTvGE+T6wDAIwTxUx9n5o1YLnYfeRUxcMLh6lS
A+gL0CI3KmjACWG/lCBdUM0CC5wBmVchMkU1BXCx/nLrp7faVJz4Z66yKeR8a6FL
p2Ucp2+uBJSa01xoNaS5foZlbHsibYWRkr5DNhJTgNniuI91oj69myEo4K0ik4Ej
mzcZjW/eAARr19+4uZHOzGGa12i4lY6lano6QuT+cqVyqJcHzgg5SwM7O25wPyBP
W8uLCG1mlcn2rSCY8eUbA0fksFlJo2yQucymuQGNBGqRVCsBDADMP6Evz+NrnIPr
/TJUhlrSmTMFNegFG5vmpKsmxpZQ2bVdXozs5teuje+lbfd5aGb4AZd4qHhDWphA
Rus9yNefWv/fiJ4+8MkuougEAqKkcuQi26q3GY/PHBrGutx+mB0BnYfDFSSIfqjq
5TfCrXQSdtN34OEEbfMwW67ugGNJiOgNUxnGYVJ29bC+fTqPpKZrpq7DgawXWpTo
ML1B7MhI5n9ObnpmyvTcYchvtc0PDUMQFkZUmY9a23wpEBeQrDHhRhXK6VtnhYAR
O3f5MeYRVM9bNPIyfK7I8oYx1eT53jH7TPnwoPnBRsJE5Kw24A1PZMGwr6m9f8wb
PFZaY9BIVrjhebe6yRQNDk4EEtkO1AGZbrUQBUmDaoRlWdgLyo+dfbbqkjv7eYj4
AiC6GFo1CVbukizSU1eId8NvZ9hitJVCakhj9SjDRjuRJDuIR2ttmFifDTg6GzQy
Fn473jdluTliZ4Ii1r3Nt4Wzu7/+jFrXqfaT+n6JFtUvN8EgPB0AEQEAAYkB2AQY
AQgAQhYhBChoGxGzkONSNnVGv813A6CuN/LLBQJqkVQrGxSAAAAAAAQADm1hbnUy
LDIuNSsxLjEyLDIsMQIbDAUJA8Q/BQAKCRDNdwOgrjfyywNXDAC1es8Trsqmis6t
ZcSuDNOM2DRxKQN3QgAowRdUbaWDsHwZOjjFcGPKUN10cF0RQ+tF2hehb2nLS8OQ
wjiWzEEoVhhRW8kqjJl6XGtXw0F+ZBVpfCH1m8/VaMnxM8jtI0MQjdsgciHv8ApQ
kGUat7ItlWdJDWXaqKk8DjOsly5Sn29Hr7vX3G518wT40PHBzvu8o0ZpBqGhTKli
unkOG79uFoyfTiaXsbG3uSMe1RhUKyIgamyR/G1TI1W9d45gLQ8Mc6lAs+qUs+Op
y835p7jTUNQcEvgnmBjc3tA94+Iu/6+qdFrVBMK5q5kEgiZwl8D0YQeE6WOTKiQv
Bh+34TSHAdfMYsZN2iYSEjAb6kWoGQE9/vWC6SCG3688IeUgREnfz0b/1jmlyDmK
pPpolyFajpnQi2IYLSlD1uPRMXiEj0YzqdoBNsnpMh8ib+c/GYDN9yn7uSyXV6pK
nVQrkHhdZH+qJKvEq3gpvfTtwSiF3FHpKD7WnIcofFzRrhR9bCU=
=tJSk
-----END PGP PUBLIC KEY BLOCK-----
```

2. Contact phone: +1630-410-7900

To help us quickly verify and reproduce the issue, please include the following information in your report as much as possible:

- Product and version: Affected specific device model, SN.
- Vulnerability description: A clear description of the potential vulnerability and its potential impact.
- Steps to reproduce: Detailed, step-by-step instructions or proof-of-concept that allow us to reproduce the issue.
- Vulnerability impact: Explain the possible impact of the vulnerability.
- Your contact information: Your name, email address, or other communication methods.

4. Vulnerability Handling Procedure

We will conduct a preliminary screening immediately upon receiving the report to confirm whether it is a valid vulnerability report:

For valid vulnerability reports, we will send an acknowledgment receipt to the reporter within 2 business days, specifying the contact person, contact information, and subsequent handling process. We will maintain open and regular communication with the reporter throughout the investigation process, and promptly inform them of our progress in verifying, classifying, and remediating the vulnerability.

For invalid vulnerability reports, we will provide the reason for rejection and terminate the handling process. Invalid vulnerability reports include the following:

1. The vulnerability cannot be reproduced, and no more valid information can be obtained.
2. It is a duplicate report.
3. The vulnerability exists in a product that has been discontinued and is no longer supported.
4. The issue is not a security vulnerability or cannot be exploited at this time.
5. Other invalid situations.

5. Vulnerability Handling Period Agreement

- During the vulnerability receiving and acceptance stage, the confidentiality period will be evaluated and determined based on the vulnerability risk level, impact scope, and remediation difficulty: High-risk vulnerabilities default to 180 days of confidentiality, medium-risk 120 days, low-risk 60 days;
- Please keep the discovered vulnerability information confidential during the confidentiality period.
- It is prohibited to cause potential or actual damage to the hardware or software systems of our company and users.

6. Disclaimer and Reserved Rights

The company reserves the right to judge and handle vulnerability reports at its own discretion, including deciding whether to fix, the time for vulnerability remediation, and the time for public disclosure, and reserves the right to modify this policy at any time.

If the reporter violates the obligations stipulated in this policy and commits any of the following acts, the company will immediately terminate communication with them and reserves the right to pursue civil, administrative, and criminal liability. If this causes losses to the company and its customers, the company will demand compensation according to law:

1. Intentionally submitting false vulnerability information to interfere with the company's normal security work;
2. Reporting vulnerabilities not through the company's official channels, or disclosing vulnerability details to third parties or the public before the company completes the fix;
3. Using the reported vulnerability to carry out attacks, steal company and customer data, disrupt the normal operation of information systems, or other illegal acts;
4. Disclosing internal sensitive information provided by the company during the vulnerability handling process;
5. Using vulnerability reporting as an excuse to demand property from the company, make unreasonable requests, or use threats, coercion, or other means to interfere with the handling work;
6. Violating other obligations of this policy and refusing to rectify after being reminded by the company.