TURBO POWER SYSTEMS CYBER SECURITY REPORTING

EU Cyber Resilience Act (CRA)- Vulnerability Reporting and Handling

Our Security Commitment

Turbo Power systems (TPS) is committed to maintaining the security, resilience and integrity of its products throughout their lifecycle. We continuously work to identify and address vulnerabilities and security incidents that may pose a threat to the confidentiality, availability and integrity of our products .

Where we become aware of an actively exploited vulnerability or a significant cybersecurity incident affecting any of our products with digital elements, the issue will be promptly escalated for assessment against relevant legal and regulatory obligations, including those under the EU Cyber Resilience Act.

We evaluate security vulnerabilities through a risk-based assessment process that considers the severity and exploitability of the vulnerability, the exposure of affected products, and any potential impact on safety. Where relevant, industry-recognised scoring methodologies, including CVSS, may be used to support risk determination.

Report a Security Vulnerability

If you believe you have identified a potential security vulnerability affecting any of our products, please report it to our PSIRT:

Security reporting email: vulnerabilityreports@turbopowersystems.com

In order to assist with our assessment of a reported vulnerability, please provide as much of the following information within the content of your report:

I. Product name, model and version

II. Affected component, feature or subsystem

III. Vulnerability type or classification

IV. Steps required to reproduce the issue

V. Proof-of-concept code or supporting evidence, where available

VI. Environment and configuration details

VII. Assessment of potential impact

VIII. Exploitation requirements or attack vector

IX. Any known or suspected active exploitation

X. Relevant CVE references or identifiers

XI. Contact information for follow-up communications

Please do not include confidential, personal or sensitive information unless it is necessary to support your report.

If we require further information to enable us to investigate the reported issue, we may contact you to request additional details.

How We Assess and Handle Reports

Our Product Security Incident Response Team (PSIRT) is responsible for coordinating the receipt, assessment and handling of reported security vulnerabilities. Upon receipt of a report, our PSIRT will review the information provided, request additional information where necessary, and assess the potential impact of the vulnerability.

We aim to acknowledge vulnerability reports within 24 business hours of receipt, excluding weekends and public holidays, subject to the nature, severity and circumstances of the report.

Our next steps after investigation

If a vulnerability is confirmed, we will determine and implement appropriate mitigation measures based on the assessed risk, severity and potential impact. Corrective actions may include security patches, software updates, configuration changes, security advisories or other measures designed to reduce risk and protect affected users.

Where appropriate, we will communicate relevant information to affected customers, including details of the vulnerability, affected products or versions, available mitigations and recommended actions. Customer communications will be proportionate to the nature and severity of the vulnerability.

Responsible & Coordinated Disclosure

TPS supports responsible and coordinated vulnerability disclosure and encourages security researchers and other stakeholders to report vulnerabilities in good faith. Where appropriate, we will work with reporters to validate vulnerabilities, assess potential impacts, develop remediation measures and coordinate disclosure activities.

We will not pursue legal action against individuals who, acting lawfully and responsibly, report potential vulnerabilities, avoid privacy violations, data destruction, service disruption, and provide TPS with a reasonable opportunity to investigate and remediate the reported issue.

Any public disclosure will be managed responsibly and in a manner intended to protect customers, reduce security risks and support transparency throughout our vulnerability management process.

Record Retention

We retain records relating to vulnerability management activities including reports, investigations, assessments, remediation efforts, customer notifications, and regulatory submissions, as applicable. Our record retention and protection practices are aligned with applicable legal, regulatory, privacy, and internal governance requirements.

Looking for product support?

The security reporting contact identified on this page is intended solely for reporting potential vulnerabilities affecting any of our products.

General product support requests, technical support enquiries, and commercial matters should be directed through the "Get in Touch" section of our website or to info@turbopowersystems.com