Sympower

Responsible Disclosure Policy.

security@sympower.net

1. Purpose

Sympower takes system and data security seriously and values independent security researchers' role in improving its security posture. This Responsible Disclosure Policy (“Policy”) guides independent security researchers (hereinafter “Independent Researchers”), that are not current Sympower employees, interns or contractors, on safely reporting potential vulnerabilities. Sympower encourages responsible reporting, commits to verifying and addressing issues, and will not take legal action against Independent Researchers who report vulnerabilities in accordance with this Policy.

2. Scope

This Policy covers all internet-facing information systems, applications, or websites owned, operated, or controlled by Sympower B.V. and/or its affiliates (hereinafter “Sympower”), including any web or mobile applications hosted on those websites, including the Sympower domain and related subdomains (collectively, “Information Systems”).

This Policy also does not cover any information systems, websites, or applications that are owned, operated, or controlled by any third party, including any service provider or contractor of Sympower, even where under a Sympower domain. Independent Researchers should comply with the responsible disclosure efforts for those other systems, websites, and applications.

3. Policy

Scope of Vulnerabilities

This Policy applies to technical vulnerabilities found in our Information Systems. Examples of covered vulnerabilities include, but are not limited to, misconfigurations, Cross-Site Request Forgeries (CSRFs), privilege escalation attacks, SQL Injection, Cross-Site Scripting (XSS), and directory traversal attacks.

The following are explicitly excluded from the scope of this Policy:

- Physical security vulnerabilities (e.g., office access, hardware theft)
- Social engineering attacks against Sympower employees, contractors, or customers
- Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks
- Spam or social engineering techniques, including phishing
- Third-party applications, websites, or services that integrate with Sympower but are not owned or operated by us
- Vulnerabilities in third-party software unless they directly affect Sympower systems
- Vulnerabilities requiring physical access to a user's device
- Vulnerabilities in systems or software that are end-of-life or no longer supported

- Recently disclosed zero-day vulnerabilities (within 30 days of public disclosure) in third-party software
- Automated scanning results without demonstrated proof of exploitability
- Reports from automated vulnerability scanners without manual verification
- Missing security headers that do not lead to direct exploitation
- SSL/TLS configuration issues without demonstrated impact
- Missing cookie flags on non-sensitive cookies
- Clickjacking on pages with no sensitive actions
- CSRF on forms with no sensitive actions
- Username or email enumeration
- Presence of autocomplete attribute on web forms
- Brute force attacks or rate limiting issues without significant impact

Rules of Engagement

When conducting security research, Independent Researchers must adhere to the following rules:

Independent Researcher shall:

- Only test against accounts they own or have explicit authorization to test
- Stop testing and report immediately if the Independent Researcher accesses any user data that is not their own
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data
- Only use exploits to the extent necessary to confirm a vulnerability's presence
- Provide Sympower with a reasonable amount of time to resolve the issue before any public disclosure
- Act in good faith throughout the research and disclosure process

Independent Researcher shall not:

- Access, modify, or delete data belonging to other users
- Execute or attempt to execute denial of service attacks
- Send unsolicited messages to users, including spam or phishing attempts
- Perform testing that could degrade the operation of Sympower systems
- Test in a manner that would result in sending unsolicited messages to users
- Use automated scanning tools in a manner that generates significant traffic
- Publicly disclose vulnerability details before Sympower has had reasonable time to remediate
- Demand financial compensation in exchange for withholding vulnerability information
- Violate any applicable laws or regulations

What We Ask From You

When reporting a vulnerability, please include the following information to help us understand and address the issue efficiently:

- A detailed description of the vulnerability and its potential impact
- Step-by-step instructions to reproduce the vulnerability
- Affected systems, URLs, or endpoints
- Any tools, scripts, or proof-of-concept code used to discover or demonstrate the vulnerability
- Your assessment of the severity (Critical, High, Medium, Low)
- Any suggestions for remediation (optional but appreciated)
- Your contact information for follow-up questions

Please submit all vulnerability reports to: security@sympower.net

What You Can Expect From Us

Sympower commits to the following when Independent Researchers report a vulnerability in accordance with this Policy:

- **Acknowledgment:** We will acknowledge receipt of your report within 3 business days
- **Communication:** We will keep you informed about the progress of your report and work with you to understand and validate the issue
- **Timeline:** We will work to remediate verified vulnerabilities in a timeframe appropriate to their severity
- **Recognition:** With your permission, we will publicly acknowledge your contribution to improving our security (unless you prefer to remain anonymous)
- **No legal action:** We will not pursue legal action against Independent Researchers who discover and report vulnerabilities in accordance with this Policy
- **Coordination:** We will coordinate with you regarding public disclosure timing

Safe Harbor

Sympower considers independent security research conducted in accordance with this Policy to be:

- Authorized concerning any applicable anti-hacking laws, and we will not initiate or support legal action against the Independent Researcher for accidental, good-faith violations of this Policy
- Authorized concerning any relevant anti-circumvention laws, and we will not bring a claim against the Independent Researcher for circumvention of technology controls
- Lawful, helpful to the overall security of the Internet, and conducted in good faith

Independent Researchers are expected, as always, to comply with all applicable laws. If legal action is initiated by a third party against you and you have fully complied with this Policy, Sympower will, if requested, inform the relevant third parties that the Independent Researchers actions were conducted in compliance with this Policy, to the best of our knowledge.

If at any time Independent Researchers have concerns or are uncertain whether security research is consistent with this Policy, please submit a report through security@sympower.net before going any further.

Disclosure Policy

Sympower follows a coordinated disclosure approach:

- We request that Independent Researchers do not publicly disclose the vulnerability until we have had reasonable time to address it
- We will work with independent researchers to agree on a disclosure timeline
- If we are unable to resolve the issue within a reasonable timeframe, we will work with the Independent Researchers to determine an appropriate public disclosure date
- We reserve the right to publicly disclose vulnerabilities sooner if they are already being actively exploited or if public disclosure is necessary to protect Sympower's customers

4. Recognition

Sympower maintains a Security Acknowledgments page on our website to recognize Independent Researchers who have helped improve our security through responsible disclosure. Recognition is provided with the Independent Researcher's consent and may include:

- Name or alias of the Independent Researcher
- Date of disclosure
- Brief description of the vulnerability category

Sympower does not currently operate a paid bug bounty program. However, we deeply value the contributions of Independent Researchers and may offer recognition in different forms, solely, at our discretion.