1. Introduction

TECHTRONIC INDUSTRIES Co., Ltd. (TTI) is a fast-growing and world-leading company in power tools, accessories, hand tools, outdoor gardening tools and floor care and cleaning products. TTI specializes in providing home decoration, repair, maintenance, Products for the construction and infrastructure industries. We are committed to accelerating the change of the industry through advanced environmentally friendly rechargeable technology. Our products have a long history and are rich in characteristics. The rechargeable product platform is of high quality, excellent performance, safety and productivity. TTI is brave in innovation and is widely recognized around the world.

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to TTi. We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always acting in compliance with it.

We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

2. Reporting

If you believe you have found a security vulnerability, please submit your report to us using the following link/email: https://support.ryobitools.com/support/contact/message# or contact service centers.

In your report please include:

Vulnerability Details:

- Asset (web address, IP Address, product or service name) where the vulnerability can be observed
- Weakness (e.g. CWE) (optional)
- Severity (e.g. CVSS v3.0) (optional)
- Title of vulnerability (mandatory)
- Description of vulnerability (this should include a summary, supporting files and possible mitigations or recommendations) (mandatory)
- Impact (what could an attacker do?) (mandatory)
- Steps to reproduce. These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as sub-domain takeovers

Optional Contact Details:

- Name

- Email Address

3. What to expect

After you have submitted your report, we will initial respond to your report within 14 days and aim to triage your report within additional 5 days. We will investigate and propose a fix within additional 35 days, and then will integrate the fix with additional 36 days. By no later than 90 days after receiving the vulnerability the fix will be released. We will also aim to keep you informed of our progress.

Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Once your vulnerability has been resolved, we welcome requests to disclose your report. We would like to unify guidance to affected users, so please do continue to coordinate public release with us.

4. Guidance

Do NOT:

- Break any applicable law or regulations
- Access unnecessary, excessive or significant amounts of data
- Modify data in the Organization's systems or services
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities
- Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests
- Disrupt the Organization's services or systems