Publication of Vulnerability Disclosure Policy

Introduction

Zhiyuan Robotics is committed to the innovative integration of AI and robotics, creating world-leading general-purpose humanoid robot products and application ecosystems. Zhiyuan Robotics was established in February 2023, co-founded by several industry veterans including "Zhi Hui Jun" Peng Zhihui, with a team possessing profound core technology background, comprehensive industry management experience, and abundant industry resources

Zhiyuan Robotics has built a leading full-stack technology for humanoid robots that integrates "body and AI,", with three major robot families: Yuanzheng, Jingling, and Lingxi, covering various commercial scenarios. Zhiyuan Robotics has taken the lead globally in achieving the mass production and commercialization of humanoid robots, with products sold to many countries and regions worldwide

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to us (the

"Organization"). 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.

Reporting

If you believe you have found a security vulnerability, please submit your report to us using the following link/email:

security@agibot.com

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

What to expect

After you have submitted your report, we will respond to your report within 5 working days and aim to triage your report within 10 working days. 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.

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