Coordinated Vulnerability Disclosure Policy

1. Introduction 引言

AgiBot Innovation(Shanghai) Technology Co.,Ltd. is committed to the security of our products and the people who rely on them. We welcome reports of potential security vulnerabilities from security researchers, customers and members of the public. This Coordinated Vulnerability Disclosure (CVD) policy explains what is in scope, how to report a vulnerability to us, how we will respond, and how we coordinate public disclosure.

智元创新（上海）科技股份有限公司致力于保障我们产品及依赖这些产品的人员的安全。我们欢迎安全研究人员、客户和公众报告潜在的安全漏洞。本协调漏洞披露（CVD）策略说明了适用范围、如何向我们报告漏洞、我们将如何响应，以及我们如何协调公开披露。

2. Scope 范围

This policy applies to the following products and services: Robot Products (including full-size humanoid robots, semi-sized humanoid robots, industrial robots, quadruped robots, commercial cleaning robots, dexterous hands, robot main control systems, safety control modules, and local operating systems, robot middleware, control algorithms, and AI models), Terminal Devices, Mobile Applications and APK, Cloud Platforms and Backend Systems, Key Security Scenarios.

本策略适用于以下产品和服务：机器人产品（包括全尺寸人形机器人、半尺寸人形机器人、工业机器人、四足机器人、商业清洁机器人、灵巧手、机器人主控系统、安全控制模块，以及本地操作系统、机器人中间件、控制算法和 AI 模型）、终端设备、移动应用和 APK、云平台和后端系统、重点安全场景。

Eligibility for remediation: products and services receive security fixes while they are within their defined support period. For example, a product is not eligible to receive remediation once it is beyond its published end-of-support date.

修复资格：产品和服务在其既定支持周期内可获得安全修复。例如，产品一旦超出其公布的支持终止日期，即无资格获得修复。

The following are out of scope : third-party services we do not operate; findings that are already public; vulnerabilities already discovered internally;reports with no demonstrable security impact; volumetric denial-of-service testing; and social-engineering of our staff or customers.

以下内容不在范围之内：我们不运营的第三方服务；已经公开的发现；内部已经发现的漏洞；无法证明具有安全影响的报告；大流量拒绝服务测试；以及针对我们员工或客户的社会工程。

3. How to report a vulnerability 如何报告漏洞

Please report potential vulnerabilities through one of the following channels:

请通过以下渠道之一报告潜在漏洞：

· Email: psirt@agibot.com.

· 电子邮件：psirt@agibot.com。

· Telephone: 400 186 0818 , via our customer service, for those who cannot use a written channel.

· 电话：400 186 0818，通过我们的客户服务，供无法使用书面渠道者使用。

We provide more than one channel so that reporters can choose a method that suits them, including by telephone where a written channel is not accessible.

我们提供不止一种渠道，以便报告者选择适合自己的方式，包括在书面渠道不可用时通过电话报告。

4. Secure and anonymous reporting 安全与匿名报告

To protect sensitive vulnerability information while it is being exchanged:

为在交换过程中保护敏感的漏洞信息：

· Vulnerability reports shall be submitted through the official reporting channel designated by AgiBot.

· 漏洞报告应通过智元指定的官方报告渠道提交。

· Where a mailbox is used, AgiBot shall ensure appropriate security measures for transmission and access control.

· 如使用邮箱，智元应确保传输安全和访问控制等适当保护措施。

· Where a PGP/GPG public key is made available, reporters are encouraged to encrypt sensitive vulnerability information before submission.

· 如智元后续提供 PGP/GPG 公钥，建议报告人在提交前对敏感漏洞信息进行加密。

You may report anonymously. If you would like a response, please give us a contact address or an alias.

您可以匿名报告。若希望得到回复，请向我们提供联系地址或别名。

We will still accept reports sent through less secure channels . Please do not let the lack of encryption stop you from reporting.

我们仍会接受通过较不安全渠道发送的报告——请不要因为缺少加密而放弃报告。

PGP key details PGP 密钥详情

We encourage finders to use encrypted communication channels to protect the confidentiality of vulnerability reports. Our PGP public key is available at the following link:

我们鼓励漏洞发现者使用加密通信渠道，以保护漏洞报告的保密性。我们的PGP公钥可通过以下链接获取：

<PSIRT PGP Key for Agibot Psirt>

<Agibot 产品安全事件响应团队 PGP 密钥>

Note: Agibot can exchange encrypted email with you using PGP and GPG

注意：Agibot 可使用 PGP 和 GPG 与您交换加密电子邮件。

5. What to include in your report 报告中应包含的内容

To help us validate and fix the issue quickly, please include as much of the following as you can:

为帮助我们快速验证和修复问题，请尽可能多地包含以下内容：

· Product identification - the affected product or service name, the affected version(s), and the platform or environment (OS, hardware) where applicable.

· 产品标识——受影响的产品或服务名称、受影响的版本，以及平台或环境（操作系统、硬件，如适用）。

· Vulnerability description - what the issue is and where it exists, and its type or class (e.g., buffer overflow, SQL injection, improper authentication).

· 漏洞描述——问题是什么、存在于何处，及其类型或类别（例如缓冲区溢出、SQL 注入、不当鉴权）。

· Impact - the potential impact if the issue is exploited (confidentiality, integrity or availability), and a severity assessment or CVSS score if you have one.

· 影响——问题被利用时的潜在影响（保密性、完整性或可用性），以及严重性评估或 CVSS 分值（如有）。

· Reproduction steps - step-by-step instructions to reproduce the issue, and proof-of-concept code or technical evidence if available.

· 复现步骤——复现该问题的分步说明，以及概念验证代码或技术证据（如有）。

· Discovery information - the date you found the issue and how (testing method, tool, or accidental finding).

· 发现信息——您发现问题的日期及方式（测试方法、工具或偶然发现）。

· Your contact information - your name or alias (you may remain anonymous) and a channel for follow-up.

· 您的联系信息——您的姓名或别名（可匿名）以及用于后续跟进的渠道。

· Disclosure intent - whether you intend to publish your findings, and any date you are working toward.

· 披露意向——您是否打算公开您的发现，以及您所争取的任何日期。

6. What you can expect from us 您可期待我们做到

After you submit a report, we will:

在您提交报告后，我们将：

· acknowledge receipt within 5 days and assign a tracking reference;

· 在5日内确认接收并分配跟踪编号；

· aim to triage and validate your report within 10 days, and contact you if we need more information;

· 力争在10日内对您的报告进行定级和验证，并在需要更多信息时与您联系；

· keep you informed of our progress at reasonable intervals;

· 以合理的间隔让您了解我们的进展；

· aim to deliver a resolution within 90 days, depending on complexity and any third parties involved;

· 视复杂程度及所涉任何第三方而定，力争在90天内交付解决方案；

· notify you when the vulnerability has been remediated, and may invite you to confirm that the fix resolves it.

· 在漏洞被修复时通知您，并可能邀请您确认该修复已解决问题。

7. Coordinated disclosure 协调披露

We follow a coordinated disclosure approach:

我们采用协调披露的方式：

· We ask that you give us a reasonable opportunity to remediate the issue before disclosing it publicly.

· 我们请您在公开披露之前给予我们合理的机会来修复问题。

· We will not publicly disclose details of a reported vulnerability before it has been addressed; any public disclosure will be coordinated and agreed between you and us.

· 在所报告的漏洞被处理之前，我们不会公开披露其细节；任何公开披露都将由您与我们协调并达成一致。

· Where appropriate we agree an embargo period. Embargo timelines can be adjusted case by case by mutual agreement, including where a coordinator or other vendors are involved.

· 在适当情况下，我们会约定禁披期。禁披时限可在双方同意的情况下逐案调整，包括在涉及协调者或其他供应商时。

· When a fix is released, we publish a security advisory and, where appropriate, request a CVE identifier and submit the information to the EU Vulnerability Database (EUVD).

· 在发布修复时，我们会发布安全公告，并在适当情况下申请 CVE 编号并将信息提交至欧盟漏洞数据库（EUVD）。

8. Where to find our security advisories 在何处查找我们的安全公告

When a vulnerability has been remediated, we publish a security advisory so that users can assess whether they are affected and how to update. You can find our advisories at:

当漏洞被修复后，我们会发布安全公告，以便用户评估自身是否受影响以及如何更新。您可在以下位置找到我们的公告：

· AgiBot official website.

· 智元官方网站。

· Product release notes, update notifications, or product update channels.

· 产品发布说明、更新通知或产品更新渠道。

· CVE records, where a CVE has been assigned, and applicable vulnerability databases.

· 在已分配 CVE 的情况下，可通过 CVE 记录以及适用的漏洞数据库查询。

9. Confidentiality保密

We treat vulnerability reports as confidential and uses the information only for vulnerability verification, coordination, remediation, notification, and legally required activities.AgiBot will not share the reporter’ s personal information with third parties without the reporter’ s explicit consent, except where required by law or necessary for coordinated vulnerability handling.

我们将漏洞报告视为保密信息，仅将相关信息用于漏洞验证、协调、修复、通知以及法律法规要求的活动。未经报告人明确同意，智元不会向第三方共享报告人的个人信息，法律法规要求或协调漏洞处理所必需的情形除外。

10. Safe harbour and good-faith research 安全港与善意研究

If you make a good-faith effort to comply with this policy during your research, we will consider your research authorised, we will work with you to understand and resolve the issue quickly, and we will not pursue or support legal action against you.

若您在研究过程中善意努力遵守本策略，我们将视您的研究为获得授权，将与您合作以迅速理解和解决问题，并且不会针对您提起或支持法律诉讼。

Good-faith research means, among other things, that you:

善意研究尤其意味着您：

· only interact with systems or accounts you own or have explicit permission to test;

· 仅与您拥有或获明确许可进行测试的系统或账户交互；

· avoid privacy violations, destruction of data, and any degradation of our services (for example, no denial-of-service testing);

· 避免侵犯隐私、破坏数据以及对我们服务造成任何降级（例如不进行拒绝服务测试）；

· access only the minimum data necessary to demonstrate the issue, and do not store, share or use it;

· 仅访问证明该问题所必需的最少数据，且不予存储、共享或使用；

· give us a reasonable time to resolve the issue before any disclosure.

· 在任何披露之前给予我们合理的时间来解决问题。