

翌视科技（宁波）有限公司

YISHI TECHNOLOGY (NINGBO) CO., LTD.

协调漏洞披露政策

Coordinated Vulnerability Disclosure Policy

文档编号: YS-SEC-CVD-001

版本号: V1.0

发布日期: 2026 年 8 月 24 日

生效日期: 2026 年 9 月 1 日

密级: 公开

编制部门: 信息安全部

1 目的与范围

翌视科技（宁波）有限公司（以下简称“翌视科技”或“公司”）重视产品与服务的信息安全。本政策旨在建立一套规范化的协调漏洞披露（Coordinated Vulnerability Disclosure, CVD）机制，为安全研究人员、客户和第三方提供清晰的漏洞报告渠道、响应时效承诺和协调披露规则。

本政策符合欧盟《网络韧性法案》（Cyber Resilience Act, CRA）第 13 条关于协调漏洞披露的要求，并参考 ISO/IEC 29147、《网络安全漏洞披露》标准制定。

2 适用范围

2.1 产品范围

本政策适用于翌视科技以下产品线的硬件、固件、软件及配套工具：

- YS3D 系列 3D 线激光相机（包含各型号感测头及控制器）
- 固件（Firmware）及嵌入式操作系统
- GenICam/GigE Vision 通信协议实现
- YiShi SDK 及配套软件工具（包括标定软件、点云处理工具等）
- 云平台服务及 Web 管理界面（如适用）

2.2 人员范围

本政策适用于以下人员向公司报告安全漏洞的场景：

- 独立安全研究人员（Security Researchers）
- 客户与合作伙伴
- 第三方安全服务机构（如渗透测试公司）
- 其他发现安全问题的任何个人或组织

3 术语与定义

术语	英文	定义
CVD	Coordinated Vulnerability Disclosure	协调漏洞披露，漏洞发现者与厂商协调处理并在补丁发布后公开披露的流程
CVSS	Common Vulnerability Scoring System	通用漏洞评分系统，用于评估漏洞严重程度（0-10 分）
漏洞	Vulnerability	产品中可被利用的安全缺陷，可能导致未经授权访问、数据泄露或服务中断

术语	英文	定义
PoC	Proof of Concept	漏洞验证代码或流程，用于证明漏洞可被利用
安全港	Safe Harbor	对善意报告漏洞的研究人员提供法律保护的声明
SBOM	Software Bill of Materials	软件物料清单，列出产品依赖的所有软件组件

4 漏洞报告渠道

安全研究人员可通过以下渠道向翌视科技报告安全漏洞：

4.1 安全邮箱

邮箱地址：security@yishi-tech.com

该邮箱由信息安全部专人维护，确保漏洞报告能够及时被接收和处理。报告人可使用 PGP 加密通信以保护敏感信息（详见 4.3 节）。

4.2 在线报告表单

公司官网安全页面提供在线漏洞报告表单，支持附件上传。表单地址详见官网 [/security](#) 页面。

4.3 PGP 加密通信

为保护漏洞报告内容在传输过程中不被截获，公司提供 PGP 公钥加密通信：

- (1) 公钥邮箱：security@yishi-tech.com
- (2) 密钥指纹（Fingerprint）：详见官网安全页面
- (3) 使用方法：报告人使用公钥加密邮件内容，公司使用私钥解密阅读

5 漏洞报告格式要求

为帮助我们快速理解和验证漏洞，建议报告包含以下信息：

字段	必填/选填	说明
产品型号	必填	如 YS3D-128-0.5、YS3D-640-10 等
固件版本	必填	当前运行的固件版本号
SDK/软件版本	选填	如使用的 YiShi SDK 或 GenICam SDK 版本
漏洞标题	必填	一句话概括漏洞性质
漏洞详细描述	必填	包含受影响的接口、协议或功能模块

字段	必填/选填	说明
复现步骤	必填	完整的复现流程，含网络环境配置
影响评估	选填	报告者自行评估的影响范围和后果
CVSS 评分	选填	报告者的自行评分（供参考）
PoC 代码/截图	选填	漏洞验证代码或截图
联系信息	必填	报告人邮箱或其他联系方式

6 漏洞严重性评估标准

公司采用 CVSS v3.1（Common Vulnerability Scoring System）作为漏洞严重性评估标准，分为以下等级：

等级	CVSS 分数	示例（3D 线激光产品）
严重 (Critical)	9.0 – 10.0	远程代码执行、未授权访问工业控制网络
高危 (High)	7.0 – 8.9	固件漏洞可获取激光校准数据或操作权限
中危 (Medium)	4.0 – 6.9	需要局域网内访问权限才能利用的信息泄露
低危 (Low)	0.1 – 3.9	仅影响本地配置文件或非核心功能
信息 (Info)	0.0	不直接构成安全风险的建议性信息

典型的 3D 线激光产品安全风险场景包括但不限于：

- (1) 通过 GigE Vision 协议未授权访问相机控制接口
- (2) 固件漏洞导致激光校准数据被篡改，影响测量精度
- (3) SDK 中的输入验证缺陷可能导致客户系统被入侵
- (4) 网络接口未加密导致测量数据被窃取

7 响应时效承诺

公司承诺按以下时效响应漏洞报告：

阶段	严重/高危	中危	低危
确认收到	24-48 小时	72 小时	7 个工作日
初步评估结果	5 个工作日	10 个工作日	14 个工作日
修复计划通报	7 个工作日	30 个工作日	90 个工作日

阶段	严重/高危	中危	低危
补丁/固件更新发布	30 个工作日	90 个工作日	180 个工作日
公开披露	补丁发布后 90 天	补丁发布后 90 天	补丁发布后 90 天

如漏洞正被主动利用，公司将启动紧急响应流程，上述时效可能缩短。涉及 CRA 第 14 条报告义务的场景，公司将在法定时限内向 ENISA/CSIRT 报告。

8 协调披露规则

8.1 披露流程

1. 报告人通过上述渠道向公司提交漏洞信息，并暂不公开披露。
2. 公司确认收到并开展初步评估，与报告人保持沟通。
3. 公司完成漏洞验证、开发补丁并发布更新。
4. 补丁发布后 90 天，报告人可以公开披露漏洞细节。
5. 公司同步发布安全公告（Security Advisory），说明漏洞性质、影响范围和修复方案。

8.2 披露时间约定

1. 默认披露期：补丁发布后 90 天。
2. 若漏洞正被主动利用，双方协商可缩短披露期。
3. 若公司在接到报告后 180 天内未发布补丁，报告人有权自行公开披露，但应提前 30 天通知公司。
4. 任何时间调整均需双方书面同意。

9 安全港声明

翌视科技承诺对符合以下条件的善意安全研究行为不采取法律行动：

1. 研究人员在发现漏洞后及时通过本政策规定的渠道报告公司。
2. 研究过程中未对公司系统、用户数据或第三方造成实际损害。
3. 研究人员未利用漏洞进行未经授权访问、数据窃取或破坏行为。
4. 研究人员未将漏洞信息提供给任何第三方（在协调披露期内）。

符合上述条件的研究行为被视为善意行为，公司不会对相关研究人员发起法律追诉或投诉。

10 政策更新与联系

本政策由信息安全部负责维护，将根据法规变化、产品更新和安全实践发展定期修订。重大变更将在公司官网安全页面公告。

安全联系邮箱: security@yishi-tech.com

公司官网安全页面: <https://www.yishi-tech.com/security>

附录: 文档修订记录

版本	日期	修订内容	修订人
V1.0	2026-08-24	初始发布	信息安全部