MEGMEET

产品安全问题控制程序

M-3-WI-RD-027

编制：潘奇银	版本状态：V1.0
审核：吴琼、陈光华	控制状态：受控文件
批准：任向阳	秘密等级：内部公开

文件更改记录

序号	版本号	修改摘要	修 改 人	批 准 人	发布日期
1	V1.0	初次发布	潘奇银	任向阳	2026-06-27

目 录

1. 目的

建立符合 IEC 62443-4-1:2018 Practice 6 要求的系统化安全问题管理机制，确保所有安全相关问题（漏洞、缺陷、事件）被**及时登记、评估、修复、验证、关闭并持续改进。

2. 适用范围

适用于公司所有面向工业控制系统环境交付的产品及其组件，包括但不限于：

- 嵌入式设备
- 工程配置软件、HMI
- 控制器固件
- 设备驱动程序
- 中间件、操作系统定制层
- 使用的第三方开源组件与库

3. 术语与定义

术语	定义
补丁	为修复安全漏洞或功能缺陷所发布的软件或固件更新。
安全更新	包含漏洞修复、风险缓解措施或安全增强功能的软件更新。
安全相关问题	指影响产品保密性、完整性或可用性的缺陷、漏洞或配置错误，包括源代码缺陷、设计缺陷、第三方组件漏洞、安全配置不当等。
安全事件	实际发生的违反安全策略或引发安全后果的事件，例如攻击者入侵、恶意篡改、数据泄露等。
安全问题单	用于记录单个安全问题从发现、评估、修复、验证到关闭全生命周期的管理表单，具备唯一标识编号
验证测试	对修复后的系统或组件执行的安全性确认测试，确保修复有效且未引入新的问题
CVE	通用漏洞披露编号
CVSS	通用漏洞评分系统（v3.x）
残余风险接受单	记录“暂不修复”决策及理由的审批文件
PSIRT	产品安全事件响应小组（公司内部）

4. 职责与分工

角色	职责说明
应急响应团队 PSIRT	统一接收、编号、分派、跟踪所有安全问题；组织应急响应,向用户通报补丁发布，提供部署指导
研发 RD	编写和测试补丁、确保与原功能兼容
安全测试工程师 ST	安全性、稳定性和功能验证
项目管理 PM	决策更新策略，沟通客户影响
安全委员会PSCM	审核更新记录，确保符合 IEC 62443 要求

5. 安全问题响应流程

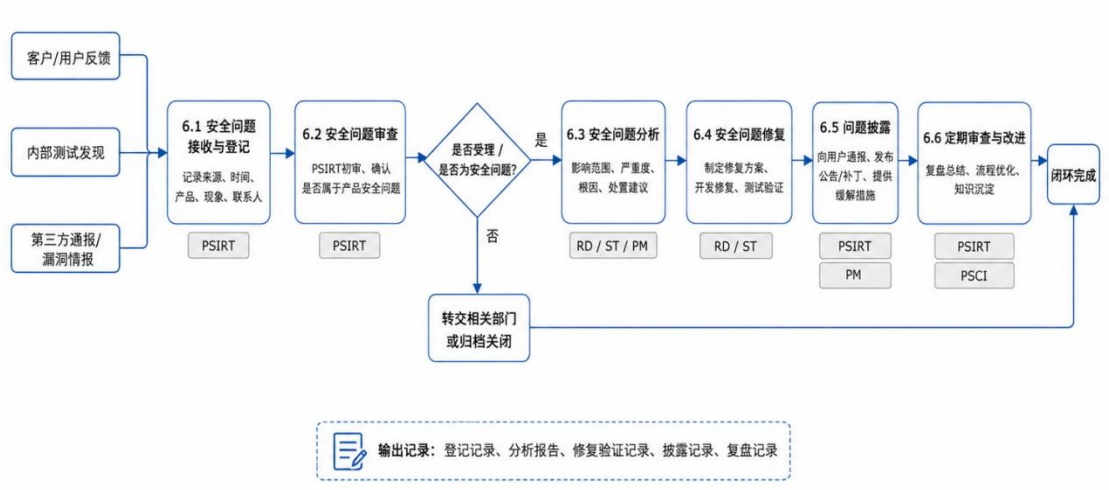

图1 安全问题控制流程图

6. 详细流程

6.1. 安全问题接收与登记

记录要求:

- 客户上报的问题（通过客服、支持通道）
- 外部安全研究人员报告（含漏洞赏金平台）
- 组件供应商通报的漏洞（如 OpenSSL、Linux 内核）

必填字段:

每一项更新事件必须进入问题数据库，包含以下字段：

- 编号
- 发现日期
- 描述
- 影响版本
- CVE 编号（如适用）
- CVSS 分数（如适用）与影响评估
- 建议缓解措施

输出物:

《安全问题单》。

6.2. 安全问题审查

- 若漏洞不在产品攻击面、配置已缓解、第三方已修复，填写《漏洞不适用性说明》并存档。
- 审查人：PSIRT + 对应开发团队；时限：1 个工作日。

输出物:

《安全问题审查报告》，PLM系统的缺陷管理系统登记。

6.3. 安全问题分析

收到并确认登记的安全问题，应由 PSIRT 牵头，组织研发、测试、安全工程师开展详细分析，至少包括以下方面：

- 影响评估

发现上下文：分析问题是在何种运行场景下被发现（如实验室测试、渗透测试、客户现场），评估其在实际环境中的可利用性与影响范围。

产品安全上下文：结合产品的角色、部署架构、接口暴露面，分析该问题在产品安全需求中的位置与影响。

纵深防御策略：检查现有防护措施（认证机制、访问控制、隔离策略、监控告警等）是否可降低该问题的风险。

- 严重性评估

必须采用行业通用漏洞评分体系（如 CVSS v3.x）对问题打分，记录分值、向量和等级（高/中/低），并在缺陷管理系统中存档。

- 版本和范围确认

检查本产品的所有版本、型号、配置，确认是否均受影响；

检查同一平台上的其他产品是否可能存在相同缺陷，建立“影响范围表”。

- 根本原因分析

采用系统化分析方法，确定缺陷的根本原因（设计缺陷、实现错误、第三方组件漏洞、配置缺陷等）；

记录结果，并在必要时修改开发流程或安全设计规范以防止复现。

- 相关问题识别

检查缺陷是否与以往的安全问题相关联（如同一模块反复出现、同一接口的不同漏洞）；将相关问题关联在缺陷管理系统中，方便追踪和综合修复。

使用 CVSS v3.x 标准进行初步评估，并考虑以下因素：

评估维度	内容说明
CVSS 分数	高于 7.0 为高危，需优先处理
利用难度	是否易于远程利用
影响范围	影响单一设备或所有部署系统
是否在野利用	有公开漏洞利用代码
客户影响	是否影响关键行业客户、是否有 SLA 要求

响应时限建议：

优先级	响应时间	发布时间
高	24 小时内分析	10 个工作日内发布
中	3 天内分析	20 个工作日内发布
低	5 天内分析	可随版本周期发布

输出物:

《安全问题分析报告》

《问题跟踪表》

6.4. 安全问题修复

处置选项

根据问题分析结果，每个问题必须选择以下处置方式之一，并在缺陷管理系统中记录：

- 修复：进入安全更新控制流程。针对问题进行修复；
- 延期处理：推迟到未来版本解决，必须记录原因和风险；
- 不修复：若残余风险低于公司接受标准，允许关闭但需审批备案。

残余风险接受：

公司定义可接受的残余风险等级（例如：低风险/低影响的漏洞在有缓解措施的情况下可以接受）；残余风险评估需基于 CVSS 评分、产品安全上下文、纵深防御策略，若决定不修复，须填写《残余风险接受单》并由安全委员会审批。

信息传递:

若问题影响其他产品或版本，必须在问题单中通知相关项目负责人并建立跨产品跟踪;

若问题来自第三方组件，需通知组件供应商，并在安全公告中注明受影响的第三方。

预防与改进:

在问题解决后，PSIRT 应总结经验，提出预防类似问题再次发生的措施;

必要时修订《安全开发流程》《安全设计规范》或对开发团队开展专项培训。

定期审查:

PSIRT 必须定期审查未关闭的安全问题，确保跟进及时;

审查频率至少为 每次产品发布或每个迭代周期一次，并形成会议纪要和更新后的问题清单。

所有安全问题修复或补丁在发布前必须完成验证与确认，验证范围覆盖需求、设计安全、实现、验证/确认及缺陷管理活动，确保修复有效且未引入新问题。未经验证闭环的问题或补丁不得发布。

输出物:

《残余风险接受单》，《漏洞不适用性说明》，《未解决问题定期审查报告》

6.5. 问题披露

披露原则:

- 遵循 “最小可用信息” 原则：在修复补丁可用前，避免披露可被恶意利用的细节。
- 遵循 负责任披露（Responsible Disclosure）流程：与漏洞发现者、合作伙伴和客户同步信息，确保修复措施可用后再公开漏洞细节。
- 所有披露过程需符合企业《信息发布管理制度》，经过 PSIRT 审核并归档。

披露方式:

- 内部披露：在修复完成前，将漏洞情况通报给相关研发、测试和支持部门，确保内部知情和协作。
- 外部披露：通过 安全公告（Security Advisory）、客户支持门户、邮件通告及合作渠道发布；若漏洞严重且影响范围广，可同步至国家/行业漏洞库（如 CNVD、CERT）。
- 向漏洞报告方反馈：在确认漏洞并完成修复前，保持与安全研究人员、供应商或客

户的沟通，说明处理进度。

披露内容：

- 漏洞基本信息：描述、CVE 编号（如有）、影响产品与版本
- 严重性与风险说明：CVSS 分数、影响范围、是否有在野利用
- 修复与缓解措施：可用补丁、配置规避措施、临时安全建议
- 时间线：发现日期、确认时间、补丁发布时间
- 联系方式：安全应急响应团队（PSIRT）联系方式，提供技术支持渠道

第三方组件漏洞策略：

- 若漏洞来源于第三方组件，PSIRT 应：
- 监控供应商通告时间；
- 若供应商提前公开披露，应在最短时间内向本产品用户同步通报受影响情况和临时缓解措施；
- 将该漏洞纳入产品缺陷管理系统，跟踪到修复闭环。

披露时限要求：

- 高危漏洞：补丁发布后 24 小时内发布公告
- 中危漏洞：补丁发布后 3 个工作日内发布公告
- 低危漏洞：随版本周期统一公告

存档与合规：

- 所有披露记录需进入问题数据库，附带公告编号、发布渠道与发布时间。

输出物：

《安全问题披露报告》

6.6. 定期审查与改进

公司 PSIRT 每年至少开展一次 安全问题管理流程的定期审查，由研发、安全、质量部门共同参与；

审查内容包括：

自上次审查以来已登记、处理和关闭的所有安全问题；

评估流程在完整性（是否覆盖 DM-1~DM-5）、效率（响应与修复时效性）以及有效性（是否真正解决问题）方面的表现；

确认所有问题均得到妥善处理或风险接受文件；

审查结论需形成相关文件，由安全委员会批准，并作为改进输入。

输出内容：

《安全问题审查报告》，用于确认项目在关键阶段是否完成预定成果与安全活动，确保每个阶段在进入下一环节前实现评审闭环和风险受控。

《未解决问题定期审查报告》，用于对产品或系统开发生命周期中尚未解决的安全缺陷和漏洞进行定期审查，评估其当前状态、潜在风险和影响，确保高优先级问题得到及时跟进。

附 录 A

（资料性）

阶段输出文件附录

序号	文件名	编制/审核/审批
1	《安全问题单》	PSIRT/项目管理 PM/安全委员会 PSCM
2	《安全问题审查报告》	研发 RD/项目管理 PM/安全委员会 PSCM
3	《问题跟踪表》	研发 RD/项目管理 PM/信息安全评审组
4	《安全问题分析报告》	研发 RD/项目管理 PM/信息安全评审组
5	《漏洞不适用性说明》	研发 RD/项目管理 PM/信息安全评审组
6	《残余风险接受单》	研发 RD/项目管理 PM/信息安全评审组
7	《安全问题披露报告》	研发 RD/项目管理 PM/信息安全评审组
8	《信息安全问题处理报告》	研发 RD/项目管理 PM/信息安全评审组
9	《安全更新说明》	研发 RD/项目管理 PM/信息安全评审组
10	《未解决问题定期审查报告》	研发 RD/质量管理 QA/信息安全评审组