

PR #45253 完整报告

vllm-project/vllm

docs: add fix disclosure policy to SECURITY.md

合并时间: 2026-06-11 20:48

原文链接: <http://prhub.com.cn/vllm-project/vllm/pull/45253>

执行摘要

- 一句话: SECURITY.md 新增安全修复披露策略
- 推荐动作: 值得快速阅读, 了解 vLLM 项目的安全响应流程。对于安全研究人员和贡献者来说, 这是一份必要的参考文档。

功能与动机

为了明确告知安全研究人员和社区贡献者, vLLM 项目对不同严重级别的安全漏洞采取不同的修复流程。高严重级别 (CRITICAL/HIGH) 的漏洞会在私有安全分支中开发修复, 并协调预通知组后再公开披露; 而中低严重级别 (MODERATE/LOW) 的漏洞则直接作为公开 PR 提交。这样既保护了高风险的漏洞细节, 又加速了低风险修复的社区 review 和采纳。

实现拆解

在 SECURITY.md 文件中新增了“Fix disclosure policy”小节, 位于安全等级分类与预通知策略之间。该小节包含一个分点列表, 说明 CRITICAL/HIGH 与 MODERATE/LOW 两种披露方式, 并声明漏洞管理团队保留根据具体情况调整披露方式的权利。

关键文件:

- SECURITY.md (模块 安全策略; 类别 docs; 类型 documentation): 唯一变更文件, 新增了安全修复披露策略的说明文档。

关键符号: 未识别

评论区精华

无讨论, 仅维护者 approval。

- 暂无高价值评论线程

风险与影响

- 风险: 无技术风险。该 PR 仅涉及文档变更, 不修改任何代码逻辑。
- 影响: 影响范围仅限于安全策略文档的可读性和透明度, 对用户、系统、团队无实质影响。有助于安全研究人员和贡献者理解项目的安全响应流程。
- 风险标记: 暂无

关联脉络

- 暂无明显关联 PR