# PR #21789 完整报告

sgl-project/sglang

Fix CVEs in Docker image: pillow, linux-libc-dev, and broken sgl-model-gateway build

合并时间：2026-04-01 11:07

原文链接：http://prhub.com.cn/sgl-project/sglang/pull/21789

## 执行摘要

此 PR 修复了 Docker 镜像中的多个安全漏洞和构建缺陷，包括 Pillow CVE-2026-25990、linux-libc-dev 内核 CVEs 以及由于二进制重命名导致的 Rust 构建失败问题，通过依赖升级和构建流程优化，将 CVEs 从 31 个减少到 7 个，显著提升了镜像安全性，对开发和部署流程有积极影响。

## 功能与动机

本 PR 旨在解决 Docker 镜像的安全风险和构建可靠性问题。根据 PR body，动机源自三个关键发现：1) Pillow 包存在 HIGH 级别漏洞 CVE-2026-25990，需升级到 12.1.1 以上；2) linux-libc-dev 包包含 16 个内核 CVEs，需更新到最新版本；3) Rust cargo cache 因构建失败遗留了 2.6GB 带 CVE 的工件，根源是 sgl-model-gateway 二进制从 sglang-router 重命名后 Dockerfile 未同步更新，导致 cargo build --bin sglang-router 失败且清理步骤被跳过。修复这些问题是提升容器化部署安全性和稳定性的必要步骤。

## 实现拆解

所有改动集中在 docker/Dockerfile 文件中，按模块拆解如下：

- 依赖升级模块：
  - 添加 linux-libc-dev 包到框架和运行时阶段，确保内核库版本更新。
  - 升级 pillow 包，通过 RUN python3 -m pip install --upgrade "urllib3>=2.6.3" "pillow>=12.1.1" 行实现。
- Rust 构建优化模块：
  - 定义 cleanup() 函数和 trap cleanup EXIT，确保无论构建是否成功都能清理 Rust 工具链。
  - 将构建目标从 sglang-router 更新为 sgl-model-gateway，修正 cargo build 命令和二进制复制路径。 关键代码逻辑示例：

```
cleanup() { rm -rf /root/.cargo /root/.rustup ...; }
&& trap cleanup EXIT
&& cargo build --release --bin sgl-model-gateway ...
```

## 评论区精华

此 PR 未发生任何 review 讨论，无争议点或技术交锋。

## 风险与影响

风险分析：

- 依赖升级风险：pillow 和 linux-libc-dev 的新版本可能引入与现有代码的兼容性问题，但测试计划已部分验证功能。
- 构建脚本风险：trap 机制依赖于正常退出，异常场景下可能导致清理不彻底，不过测试确认了清理效果。
- 安全残留风险：仍有 7 个 CVEs 来自上游 hf-xet Go stdlib，不受本 PR 控制，需监控第三方更新。

影响分析：

- 对用户：镜像更安全、更小，构建失败问题得到解决，提升了部署体验。
- 对系统：减少了安全攻击面，镜像扫描得分改善，支持更安全的运行环境。
- 对团队：加强了 CI/CD 流程的健壮性，为后续安全扫描（如 PR #21772）奠定了基础。

## 关联脉络

本 PR 与历史 PR 存在以下关联：

- PR #14312：此 PR body 提到二进制重命名发生在此 PR，是本 PR 修复构建失败问题的根源，揭示了跨 PR 同步更新的重要性。
- PR #21772：近期历史 PR 中涉及添加 Trivy 漏洞扫描到 Docker 构建，与本 PR 的安全修复主题形成互补，共同推动仓库的安全治理趋势。整体来看，仓库正通过一系列 PR 强化安全性和基础设施可靠性。