PR #23660 完整报告

sgl-project/sglang

Fix for CVE-2026-5760

合并时间：2026-04-29 10:39

原文链接：http://prhub.com.cn/sgl-project/sglang/pull/23660

执行摘要

- 一句话：修复路由模板渲染 SSTI 安全漏洞
- 推荐动作：建议合并。这是一个典型的安全修复，变更小而精准，无需额外测试。开发者可关注 Qwen3 reranker 相关功能是否正常工作。

功能与动机

CVE-2026-5760（https://www.kb.cert.org/vuls/id/915947）表明，/v1/rerank 端点使用非沙箱化的 Jinja2 环境渲染模型提供的模板，攻击者可通过构造恶意模板实现服务端模板注入。本 PR 旨在通过沙箱化环境消除此风险。

实现拆解

1. 修改 _get_jinja_env() 函数: 在 python/sglang/srt/entrypoints/openai/serving_rerank.py 中，将 jinja2.Environment 替换为 jinja2.sandbox.ImmutableSandboxedEnvironment。新增 from jinja2.sandbox import ImmutableSandboxedEnvironment 导入。
2. 添加注释: 在新创建的环境上添加了注释 # Using a sandboxed environment to stop malicious execution during model loading.。
3. 移除旧环境: 删除了旧的 return jinja2.Environment(...) 代码块。
4. 影响范围: 仅影响 _get_jinja_env() 函数，该函数被 _render_jinja_chat_template 调用，用于 Qwen3 reranker 模板渲染。无其他功能变更。

关键文件：

- python/sglang/srt/entrypoints/openai/serving_rerank.py（模块 API 入口；类别 source；类型 dependency-wiring；符号 _get_jinja_env）：唯一变更文件，修复 SSTI 漏洞的核心改动所在。

关键符号：_get_jinja_env

关键源码片段

python/sglang/srt/entrypoints/openai/serving_rerank.py

唯一变更文件，修复 SSTI 漏洞的核心改动所在。

```
def _get_jinja_env():
    try:
```

```
        import jinja2 # Lazy import: server env should provide this dependency.
        from jinja2.sandbox import ImmutableSandboxedEnvironment # <-- 新增导入沙箱环境
    except ModuleNotFoundError as e:
        raise ValueError(
            "Rendering Qwen3 reranker prompts requires `jinja2`. "
            "Please install it in your runtime environment (e.g., `pip install jinja2`)."
        ) from e
    # Using a sandboxed environment to stop malicious execution during model loading.
    return ImmutableSandboxedEnvironment( # <-- 使用不可变沙箱环境替代普通 Environment
        loader=jinja2.BaseLoader(),
        autoescape=False,
        undefined=jinja2.Undefined,
    )
```

评论区精华

Review 由 kpham-sgl 批准，无讨论或争议。变更直接、聚焦。

- 暂无高价值评论线程

风险与影响

- 风险：变更极小（+3/-2），仅涉及 Jinja2 环境类的替换。ImmutableSandboxedEnvironment 是 Jinja2 官方沙箱，行为与普通 Environment 兼容，但限制了 __globals__ 等属性访问。风险极低，但需确认所有依赖 _get_jinja_env() 的路径（Qwen3 reranker 模板渲染）均能正常工作。未添加单元测试，但变更简单，回归风险小。
- 影响：仅影响使用 Qwen3 reranker 功能的用户，且仅限于模板渲染路径。沙箱化环境会阻止模板中的某些高级特性（如访问 os、__import__ 等），但正常模板渲染不受影响。对于依赖模板内执行任意代码的用例（极少），此项变更为破坏性变更，但符合安全最佳实践。
- 风险标记：安全修复，缺少测试

关联脉络

- 暂无明显关联 PR