Vite任意文件读取漏洞(CVE-2025-30208)复现及漏洞环境

漏洞介绍

Vite 是一个由 Evan You（Vue.js 作者）开发的前端构建工具，主打**快速启动和高效构建**。它利用原生 ES 模块特性，在开发环境下实现**即时模块热更新（HMR）**，几乎零延迟启动项目；在生产环境下则基于 Rollup 进行打包，兼顾速度与优化。Vite 支持多种框架（如 Vue、React、Svelte 等），配置简单、插件体系灵活，是现代前端开发的高效利器。

Vite 是一个前端开发工具提供者，其在 6.2.3、6.1.2、6.0.12、5.4.15 和 4.5.10 之前的版本中存在一个安全漏洞。该漏洞源于 `@fs` 原本用于拒绝访问 Vite 允许列表之外的文件，但通过在 URL 中添加 `?raw??` 或 `?import&raw??`，可以绕过这一限制并返回文件内容（如果文件存在）。绕过的原因是在多个处理环节中会移除类似 `?` 的结尾分隔符，而正则表达式在解析查询字符串时未考虑这一点，导致限制失效。攻击者可借此漏洞将任意文件内容返回到浏览器。**只有那些通过 `--host` 参数或 `server.host` 配置显式暴露 Vite 开发服务器到网络的应用会受到影响。**该问题已在 6.2.3、6.1.2、6.0.12、5.4.15 和 4.5.10 版本中修复。

漏洞条件

- = 6.2.0：<= 6.2.2
- = 6.1.0：<= 6.1.1
- = 6.0.0：<= 6.0.11
- = 5.0.0：<= 5.4.14
- <= 4.5.9

环境搭建

在上图文件夹下执行一条命令即可部署环境：

```
docker-compose up -d
```

访问 http://your-ip:5173 ， 看到如下页面表示环境搭建成功

漏洞对比

Vite 默认只允许访问项目根目录（ `root` ）下的文件。但是在某些高级用法中，开发者可能需要访问项目根目录之外的文件，比如使用本地绝对路径，这时就用到了 `@fs` 。

在几年前的CNVD-2022-44615（Vite任意文件读取漏洞）中，访问 `/@fs/etc/passwd` 即可读取到 `/etc/passwd` 文件。

Unrestricted directory traversal with `@fs` #2820

Closed #3784, #2850

GrygrFlzr opened on Apr 2, 2021

Describe the bug

The entire filesystem is indiscriminately exposed while the Vite dev server is running. Combined with the fact that the server is exposed to `0.0.0.0` by default, you're effectively opening your machine to the world during development.

This is technically a Vite *feature* as currently documented, but probably not actually intended.

Reproduction

Any Vite project will do.

```
npm init @vitejs/app app
cd app
npm install
npm run dev
```

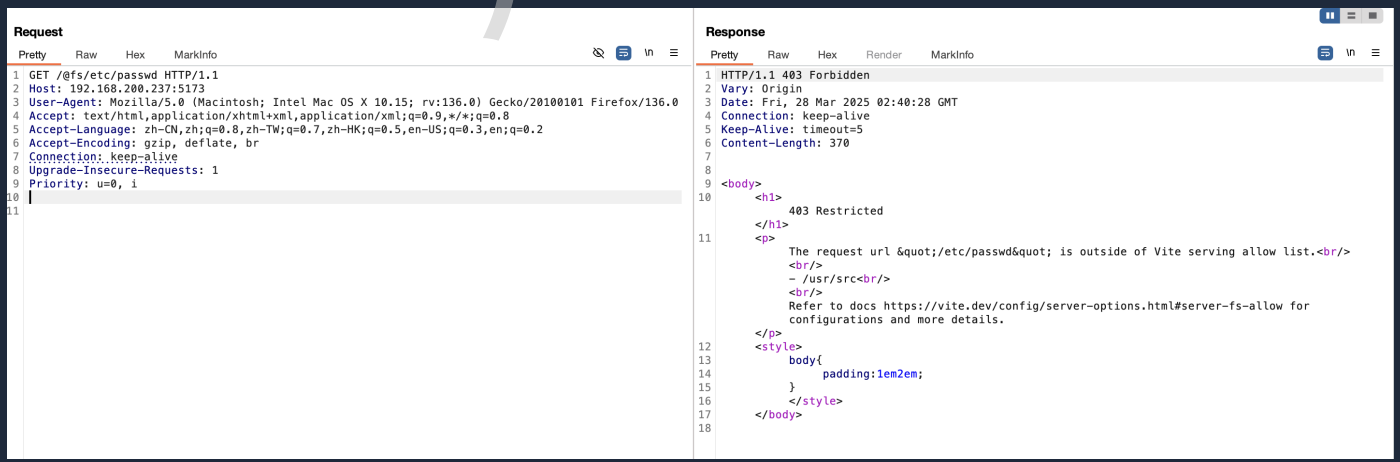
- If running on Windows, visit http://localhost:3000/@fs/windows/debug/netsetup.log
- If running on Linux, visit http://localhost:3000/@fs/etc/passwd
- No idea of an equivalent on macOS but I'm sure you can think of something

Combined with the fact that any "out of root" directories already reveal the username of the current user, you can also easily do http://localhost:3000/@fs/home/username/.ssh/id_rsa

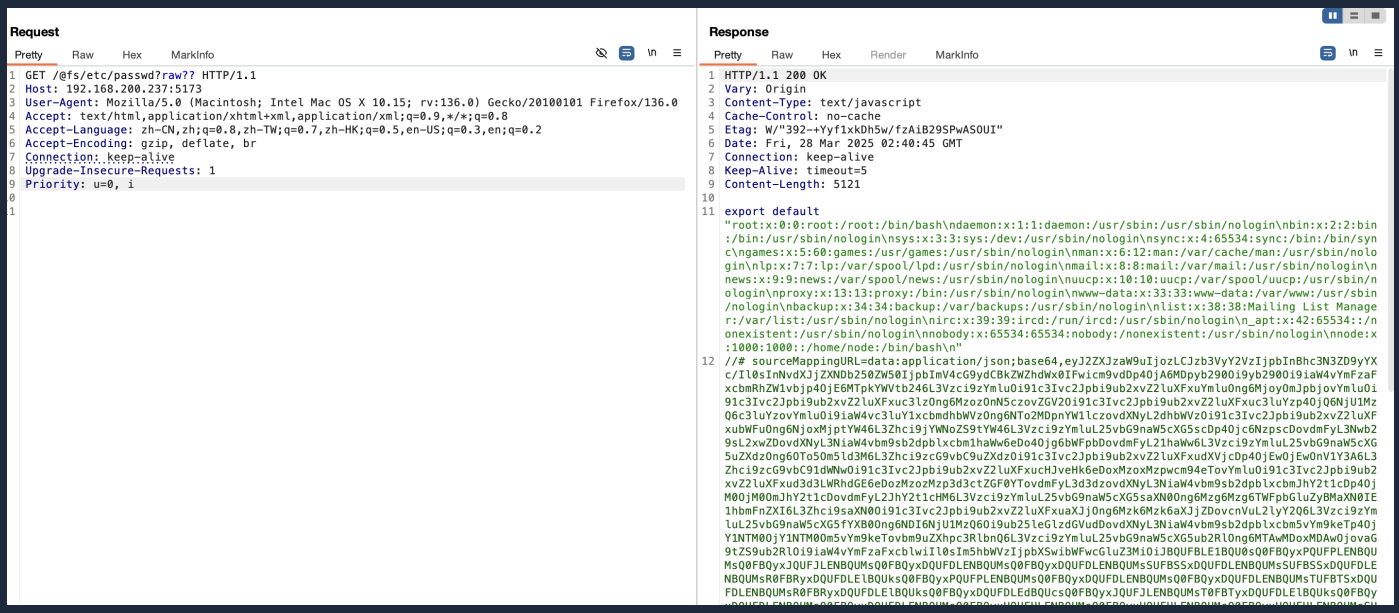
System Info

漏洞复现

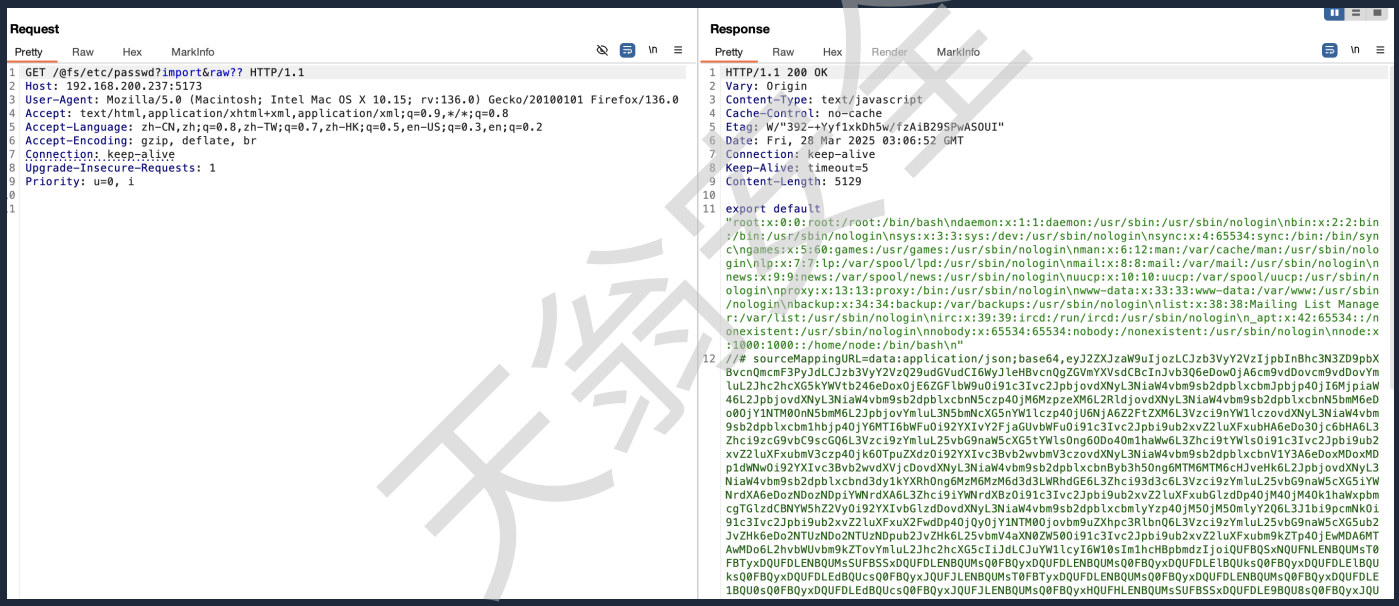
我们尝试像CNVD-2022-44615一样访问 `/@fs/etc/passwd`，发现已经被403禁止访问了



但我们尝试在 `/@fs/etc/passwd` 后添加 `?raw??` 时，发现绕过了限制成功读取到了 `/etc/passwd` 文件



在 /@fs/etc/passwd 后添加 ?import&raw?? 时，也可以绕过



漏洞修复

临时解决方案：

- 禁止在生产环境开放 Vite Dev Server，仅限本地或内网使用。
- 在防火墙或代理层配置 IP 白名单，限制仅可信地址访问 Dev Server。
- 在代理层拦截含 /@fs/ 、 ?raw 、 ?import&raw 的请求，防止绕过访问本地文件系统。

解决方案：

- 对于Vite = 6.2.0：升级到 6.2.2 以上版本
- 对于Vite = 6.1.0：升级到 6.1.1 以上版本
- 对于Vite = 6.0.0：升级到 6.0.11 以上版本
- 对于Vite = 5.0.0：升级到 5.4.14 以上版本
- 对于Vite <= 4.5.9：升级到 4.5.9 以上版本