# Nginx CVE-2017-7529（越界读取缓存）

# 影响版本

该漏洞影响所有 0.5.6 - 1.13.2版本内默认配置模块的Nginx只需要开启缓存攻击者即可发送恶意请求进行远程攻击造成信息泄露

(nginx会缓存静态文件 如果二次请求命中文件就会把文件中的HTTP返回包体发送给用户)

复现（没理解）

/Users/green/vulhub/nginx/CVE-2017-7529

Docker compose up -d

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

在vuln底下有poc.py

文本

描述已自动生成

执行python3 poc.py <http://127.0.0.1:8080>

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

得到响应体信息