Codiad 漏洞挖掘笔记 (0x05) [任意文件读写漏洞]

王一航 / 2017-08-30 15:38:00 / 浏览数 3938 安全技术 漏洞分析 顶(0) 踩(0)

简介：

之前做过一道CTF的题目(还是 facebook 的一个漏洞？)，具体是什么比赛忘记了
那个题目大概是让用户上传一个 tar 压缩包，然后会将其中的 txt 文件的内容显示出来
正解是先本地创建一个符号链接指向某一个敏感文件的绝对路径 (/etc/passwd)
然后使用 tar 打包后上传给具有漏洞的程序，然后，经过程序处理以后就会 follow 符号链接将文件内容显示出来
这个漏洞大概也如此

在审计和测试 Codiad 这个开源程序的时候，Codiad 开发者自己维护了一个用于展示 Codiad Demo 的网站
> demo.codiad.com

测试的时候使用了该网站进行测试

漏洞分析：

漏洞主要出现在 Codiad 打开文件的函数中，由于对打开的文件类型缺乏判断，因此可以被恶意攻击者利用

> components/filemanager/class.filemanager.php

这里在打开文件的时候并没有检查文件是否是一个符号链接文件，直接就将其内容获取并显示
这样就给了攻击者利用符号链接文件读取任意文件的机会
攻击者可以构造一个符号链接文件指向敏感文件，然后就可以利用这个文件读取到目标服务器上的任意文件

由于笔者知识储备有限，并不是很了解符号链接文件的结构，暂时还不能手动创建一个符号链接文件

但是 Codiad 提供了从 github 导入 git 仓库的功能

因此笔者找到一个这个漏洞的利用方式
就是先创建一个仓库，在仓库中创建一个符号链接文件，指向某一个敏感文件 (例如 /etc/passwd)

然后将其推送到 github

github 对符号链接文件的保护还是比较好，并没有出现类似的漏洞

最后再使用 Codiad 的从 github 导入仓库的功能将这个仓库导入
最后就直接在 Codiad 中打开这个文件即可得到这个文件的内容
利用成功截图如下：

最后又测试了一下是否可以将一整个目录作为符号链接来挂载到 Codiad 的目录中
发现确实是可以的

这里直接将 /etc 目录挂载到了 Codiad 的项目下

本地测试的时候更是直接将系统根目录直接挂载

修补方案：

[redacted] , [redacted] `is_link` [redacted]

参考资料：
> https://github.com/WangYihang/Codiad-pentest

上一篇：先知Xss挑战赛 - L3m0n ... 下一篇：Codiad 新的命令执行漏洞及 ...

1. 0 条回复
   - 动动手指，沙发就是你的了！

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板