GitBook 任意文件读取漏洞—【CVE-2017-15688】

王一航 / 2017-10-24 06:25:00 / 浏览数 4793 安全技术 漏洞分析 顶(0) 踩(0)

前言 :

漏洞已经报告给厂商 , 不过厂商并不认为这个是一个严重的漏洞
因为 GitBook 网站在编译 Markdown 的书籍的时候是在 LXC 环境下进行的
其实只是一个虚拟的环境 , 并不能读取到敏感的数据

挖掘过程 :

漏洞报告 PDF : https://drive.google.com/file/d/0B3qR_-XJ9Er3ZnhjSnFReW5PMDA/view?usp=sharing

其实过程和之前的 CVE-2017-15690 几乎一模一样

漏洞的成因都是因为没有处理好 Linux 下的符号链接文件 , 导致任意文件读取的

漏洞需求 :

首先需要攻击者需要拥有一个 GitHub 账号 , 一个 GitBook 账号 , 并且将两个账号关联 , 使 GitBook 账号可以使用 GitHub 中的仓库来创建书籍

利用步骤 :

1. 在 GitHub 上创建一个仓库
2. 将空的仓库克隆到本地
3. 使用命令在仓库中初始化一个书籍

```
gitbook init
```

1. 在仓库的某一个目录下 (或者根目录) 创建一个符号链接文件 , 例如

```
ln -s /etc/passwd ./passwd.md
```

注意后缀名必须为 .md

1. 编辑仓库根目录的 SUMMARY.md 将刚才创建的符号链接文件添加至该文件的目录结构中
1. 执行命令 , 编译该书籍

```
gitbook serve
# ■■■■■■■■ web ■■■ ■■■■■■■■■■■■
```

1. 访问发现确实读取到了本机的 /etc/passwd 文件
1. 将本地仓库提交并 push 到 GitHub, 然后在 GitBook 中就可以看到读取到的目标服务器的文件了

POC :

https://wangyihang.gitbooks.io/awesome-web-security/content/vulnerabilities/passwd.html

---

白盒分析 :

https://github.com/GitbookIO/gitbook
下载代码, 定位到解析 SUMMARY.md 的函数

判断是否是一个文件

路径清洗函数

定义 MarkDown 文件的配置文件

在黑盒测试的时候就已经发现, 符号链接文件必须是 .md 才可以

这里是读取文件的函数 , 可以看到在读取之前并没有对文件是否是符号链接文件进行判断
这样也就造成了这个漏洞

修补方案 :

在编译时 , 判断文件是否是符号链接 , 如果是则跳过对该文件的编译

点击收藏 | 0 关注 | 0

上一篇：Typecho Install.p... 下一篇：巡风系统在同程运维

1. 2 条回复

 wilsonlee1 2017-10-25 02:52:58

一句话概括 创建一个符号链接文件 ln -s /etc/passwd ./passwd.md

0 回复Ta

 hahaha 2017-10-25 07:41:47

厉害厉害 膜拜大牛

0 回复Ta

登录 后跟帖

先知社区

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