New issue

Jump to bottom

kkFileView arbitrary file deletion vulnerability #370

Closed **achiove** opened this issue on Jul 20 · 2 comments

achiove commented on Jul 20 • edited

问题描述Description

kkFileview v4.0.0存在任意文件删除漏洞，可能导致系统任意文件被删除。

kkFileview v4.0.0 has an arbitrary file deletion vulnerability, which may lead to arbitrary file being deleted.

漏洞位置vulerable code location

src/main/java/cn/keking/web/controller/FileController.java文件78行，fileName参数用户可控，由于只截取"/"后面的内容作为文件名，导致可以利用".."来实现目录遍历，导致任意文件删除漏洞。

The vulnerability code is located at line 78 in src/main/java/cn/keking/web/controller/FileController.java, the fileName parameter can be controlled by user. and it fetch the content after "/" as fileName, which leads to we can use ".." to achieve directory traverse that result in arbitrary file deletion.

```
@RequestMapping(value = "deleteFile", method = RequestMethod.GET)
public String deleteFile(String fileName) throws JsonProcessingException {
if (fileName.contains("/")) {
fileName = fileName.substring(fileName.lastIndexOf("/") + 1);
}
File file = new File(fileDir + demoPath + fileName);
logger.info("删除文件：{}", file.getAbsolutePath());
if (file.exists() && !file.delete()) {
logger.error("删除文件【{}】失败，请检查目录权限！",file.getPath());
}
return new ObjectMapper().writeValueAsString(ReturnResponse.success());
}
```

漏洞证明PoC

/deleteFile?fileName=demo%2F..\calc.pdf

get请求此uri会删除\kkFileView-master\server\src\main\file目录中的calc.pdf（原本只能删除\kkFileView-master\server\src\main\file\demo目录下的文件）

POC
/deleteFile?fileName=demo%2F..\calc.pdf
request this uri by HTTP GET method will delete \kkFileView-master\server\src\main\file\calc.pdf (which logically should delete \kkFileView-master\server\src\main\file\demo\calc.pdf)

免责声明：请勿使用漏洞在他人部署的服务上进行测试、攻击，否则所有法律责任自行承担。

achiove commented on Jul 20 Author

this vulnerability is tested on windows, and it may not exploited on unix system

gaoxingzaq commented on Jul 23

修复办法
private static Pattern FilePattern = Pattern.compile("[\\/:*?"<>|]");

```
/**
 * 路径遍历 漏洞修复
 * @param str
 * @return
 */
public static String filenameFilter(String str) {
    return str==null?null:FilePattern.matcher(str).replaceAll("");
}
```

fileName= filenameFilter(fileName);

klboke added a commit that referenced this issue on Jul 25

Fix #370 ✓ bcf9e81

klboke closed this as completed in 86960e3 on Jul 25

Assignees

No one assigned

Labels

None yet

Projects

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants