New issue

Jump to bottom

Another kkFileView XSS Vulnerability #389

Open **absolutyy** opened this issue on Sep 14 · 1 comment

absolutyy commented on Sep 14 • edited

问题描述Description
kkFileview v4.1.0存在另一处XSS漏洞，可能导致网站cookies泄露。

kkFileview v4.1.0 has another XSS vulnerability, which may lead to the leakage of website cookies.

漏洞位置vulerable code location
kkFileView/server/src/main/java/cn/keking/web/controller/OnlinePreviewController.java文件61行，errorMsg参数用户可控，传输到错误提示处理函数中处理后用于前端错误提示，整个流程未对errorMsg参数进行过滤处理

The vulnerability code is located at line 61 in kkFileView/server/src/main/java/cn/keking/web/controller/OnlinePreviewController.java , The errorMsg parameter is user-controllable. After being transferred to the error prompt processing function for processing, it is used for the front-end error prompt, and the errorMsg parameter is not filtered throughout the process

```
public String onlinePreview(String url, Model model, HttpServletRequest req) {
    String fileUrl;
    try {
        fileUrl = WebUtils.decodeBase64String(url);
    } catch (Exception ex) {
        String errorMsg = String.format(BASE64_DECODE_ERROR_MSG, "url");
        return otherFilePreview.notSupportedFile(model, errorMsg);
    }
    FileAttribute fileAttribute = fileHandlerService.getFileAttribute(fileUrl, req);
    model.addAttribute("file", fileAttribute);
    FilePreview filePreview = previewFactory.get(fileAttribute);
    logger.info("预览文件url: {}, previewType: {}", fileUrl, fileAttribute.getType());
    return filePreview.filePreviewHandle(fileUrl, model, fileAttribute);
}
```

漏洞证明PoC
官方演示站点为最新4.1.0版本，以此为演示，访问漏洞位置（url参数值需要经过base64编码和url编码）：
https://file.keking.cn/onlinePreview?
url=aHR0cHM6Ly93d3cuYmFpZHUuPGltZyBzcmM9MSBvbmVycm9yPWFsZXJ0KDEpPg==

The version of official demo site is v4.1.0. Visit
https://file.keking.cn/onlinePreview?
url=aHR0cHM6Ly93d3cuYmFpZHUuPGltZyBzcmM9MSBvbmVycm9yPWFsZXJ0KDEpPg==
and the concept is proofed. (The url parameter value needs to be base64 encoded and url encoded.)

👍 1

gaoxingzaq commented on Sep 19

\server\src\main\java\cn\keking\service\impl\OtherFilePreviewImpl
修改
public String notSupportedFile(Model model, String fileType, String errMsg) {
fileType= HtmlUtils.htmlEscape(fileType);
errMsg= HtmlUtils.htmlEscape(errMsg);
model.addAttribute("fileType", fileType);
model.addAttribute("msg", errMsg);
return NOT_SUPPORTED_FILE_PAGE;
}

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants