jQuery-File-Upload—三个漏洞的故事

niexinming / 2019-01-14 09:18:00 / 浏览数 3025 技术文章 翻译文章 顶(0) 踩(0)

翻译自：https://blog.detectify.com/2018/12/13/jquery-file-upload-a-tale-of-three-vulnerabilities/
翻译：聂心明

在github上星个数第二多的JavaScript项目中有两个远程命令执行漏洞，并且星数第三多的那个项目可能会通过jQuery-File-Upload任意删掉被上传的文件。后者是有意的行
Crowdsource已经在
jQuery-File-Upload找到三个安全漏洞了，并且这些漏洞已经被安全研究员提交了我们的社区中，并且我们已经在我们的漏扫工具Detectify中实现了检测。我们的研究员发

https://youtu.be/JXxUWj5ybUk

CVE-2018-9206 未授权任意文件上传漏洞

第一个漏洞在2015年的时候就已经被发现了。但是，在2018年的时候才被分配cve编号，并且通过《Thousands of Applications were vulnerable to RCE via jQuery File
Upload》才被大家所熟知。jQuery-File-Upload是一个开源的文件上传组件，在github上是星数第二多的JavaScript项目，星数第一多的项目是jQuery
JavaScript。CVE-2018-9206的核心问题在于服务器配置和php的组件技术，不是JavaScript的问题。当然，这个问题最后成为JavaScript的漏洞让人觉得有点不可思议，但

```
# The following directives prevent the execution of script files
# in the context of the website.
# They also force the content-type application/octet-stream and
# force browsers to display a download dialog for non-image files.
SetHandler default-handler
ForceType application/octet-stream
Header set Content-Disposition attachment

# The following unsets the forced type and Content-Disposition headers
# for known image files:
<FilesMatch "(?i)\.(gif|jpe?g|png)$">
ForceType none
Header unset Content-Disposition
</FilesMatch>

<...>
```

上面是jQuery-File-Upload的.htaccess文件，并且存在于9.22.0版本之前，为了防范文件上传漏洞。.htaccess可以设置MIME的类型为application/octet-stream，从而让
允许任意文件上传，但是不能在服务器上执行它们，因为它们信任web服务器对此做了检查。修补之后，后面的版本检查了文件的上传类型。可是问题是，在Apache的2.3.9

基于ImageTragick的远程命令执行

jQuery-File-Upload的第二个漏洞在黑客社区中被广为所知，这个漏洞一直没有被公开，因为CVE-2018-9206的出现，这个漏洞才被大家所关注，之后越来越多的人开始研
AKA ImageTragick）。这里有个演示视频。攻击者会把下面的GhostScript保存成后缀为PNG, GIF 或者JPG的文件，然后再把他们上传到服务器中。

```
%!PS
userdict /setpagedevice undef
save
legal
{ null restore } stopped { pop } if
{ legal } stopped { pop } if
restore
mark /OutputFile (%pipe%ping example.com) currentdevice putdeviceprops
```

服务器会执行ping
example.com这个指令，注意，在不同的操作系统中GhostScript可能看着会有一些不同，但是ping指令可以运行在大多数的环境中，这样就可以利用自动化的手段来发现存

一个有意为之的漏洞

第三个也是最后一个漏洞是不安全的对象引用，或者称之为 IDOR
vulnerability，一个站长报告过这个问题，但是issue中明确写着这是一种"有意的功能"，但是很多jQuery-File-Upload
用户不知道这一特性，也不知道这一特性的风险。这就是为什么：向文件上传接口发送get请求，服务器就会返回一组json数据，里面包含所有之前上传的文件。这就会暴露

```
{"files":[{"name":image.jpg","size":68549,"url":"http:\/\/example.com\/image.jpg","thumbnailUrl":"http:\/\/example.com\/thumbn
```

通过返回报文，用户就可以通过url字段的内容看到之前上传过的文件。也可以通过发送DELETE请求来删除所有的文件，发送的请求就像下面这样：

```
curl -X DELETE http://example.com/server/php?file=image.jpg
```

当我们看到网站使用jQuery-File-Upload时，就可以故意的去访问这个“有意的漏洞”了。如果这个网站是一个约会网站，用户肯定会很自然的上传自己的图片。通过发送这样
Sebastian Tschan了（jQuery-File-Upload的主要维护者），并且所有的网站都发现了这样的漏洞。

修复

最开始提到的两个漏洞已经在jQuery-file-upload后续的版本修复了。我建议大家赶紧升级到最新的版本。为了修复最后一个漏洞，你应该严格限制文件上传接口的权限（通

上一篇：区块链安全-以太坊智能合约静态分析 下一篇：区块链安全-以太坊智能合约静态分析
1. 0 条回复
   - 动动手指，沙发就是你的了！