O7-1020A-RCE

漏洞描述:

O2OA是一个基于 I2EE 分布式架构,集成移动办公、智能办公,支持私有化部署,自适应负载能力的,能够很大程度上节约企业软件开发成本,基于AGPL协议开放源代码的企业信息化系统需求定制开发平台解决方案。通过/x_program_center/jaxrs/invoke 发现 020A v6.4.7 包含一个远程代码执行(RCE)漏洞。

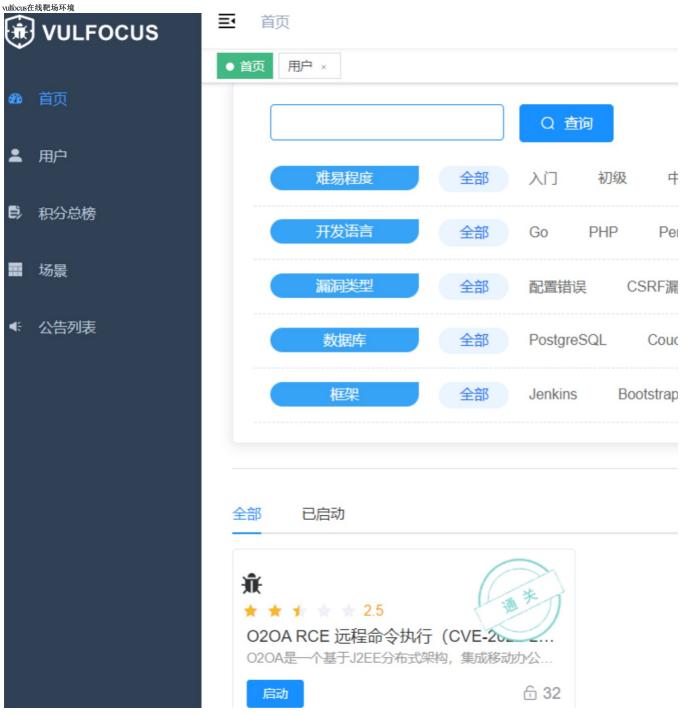
影响版本:

020A v6.4.7

网络测绘:

fofa语法:

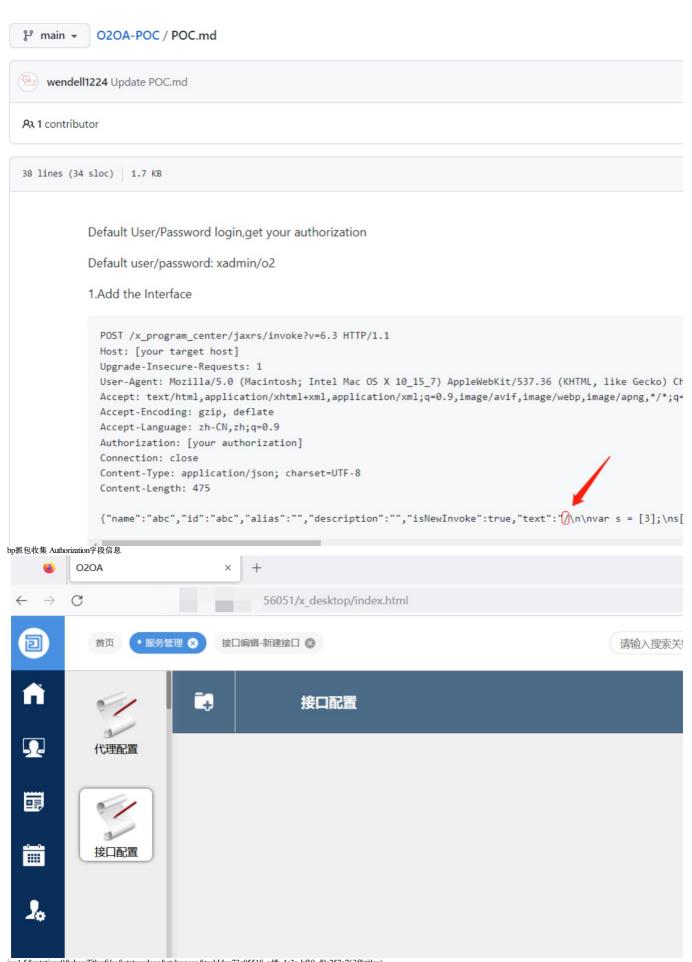
漏洞复现:



5、利用流程

1、使用默认口令xadmin/o2登录后台,利用某大佬写的POC进行复现

项目地址: O2OA-POC/POC.md at main _wendell 124/O2OA-POC - GitHub 注意事项: 大佬的POC里面应该是打错了,多打了一个 "/",所以导致添加的接口无法调用指令,删掉即可。



io = 1.5 & rotation = 0 & show Title = false & status = done & style = none & task Id = u73c05518 - adfb - 4c3a - bf19 - d9e252e763f & title = 1.5 & rotation = 0 & show Title = false & status = done & style = none & task Id = u73c05518 - adfb - 4c3a - bf19 - d9e252e763f & title = 1.5 & rotation = 0 & show Title = false & status = done & style = none & task Id = u73c05518 - adfb - 4c3a - bf19 - d9e252e763f & title = 1.5 & rotation = 0 & show Title = false & status = done & style = none & task Id = u73c05518 - adfb - 4c3a - bf19 - d9e252e763f & title = 1.5 & rotation = 0 & show Title = false & status = done & style = none & task Id = u73c05518 - adfb - 4c3a - bf19 - d9e252e763f & title = 1.5 & rotation = 0 & show Title = false & status = done & style = none & task Id = u73c05518 - adfb - 4c3a - bf19 - d9e252e763f & title = 1.5 & rotation = 0 & show Title = false & status = done & style = none & task Id = u73c05518 - adfb - 4c3a - bf19 - d9e252e763f & title = 0 & show Title = 1.5 & rotation = 0 & show Title = 1.5 & show Titl

添加一个接口



Host: [your target host]

Content-Length: 0

Accept: text/html,application/json,*/*

X-Requested-With: XMLHttpRequest

Accept-Language: zh-CN

Authorization: [your authorization]

User-Agent Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36

Content-Type: application/json; charset=UTF-8

Origin: http://[your target host]

Referer: http://[your target host]

Referer: http://[your target host]

Accept-Encoding: gzip, deflate

Cookie:

Connection: close