私有云未授权接口导致代码执行漏洞

背景

近日，金山办公安全应急响应中心（WPSSRC）监测到“私有云未授权接口导致代码执行漏洞”的相关安全情报。

我司安全技术团队第一时间启动应急响应机制，经紧急核查与分析，该漏洞仅影响通过 Docker 部署并暴露在公网的文档中台或文档中心，其他部署方式不受影响，处于物理隔离状态的私网用户亦不受影响。现将有关情况说明如下：

一、漏洞情况

文档中心和文档中台存在未授权接口漏洞，可通过向 Etcd 写入恶意路由并结合 Kubelet 匿名访问实现远程代码执行。经核实，该漏洞已在 2024 年 5 月得到修复。

(一)受影响版本

漏洞影响的产品和版本如下：

产品名称	部署方式	影响版本
文档中心	Docker	v7.0.2306b ≤ 文档中心 < v7.0.2405b
文档中台	Docker	v6.0.2205 ≤ 文档中台 < v7.1.2405

(二)漏洞等级

漏洞等级	CVSS 3.0	利用情况
严重	**10.0** (CVSS:3.0/AV:N/AC:C/PR:N/UI:N/S:C/C:H/I:H/A:H)	容易被利用

影响范围

WPS 文档中台

版本 v6.0.2205<=version<v7.1.2405。

修复脚本

fix-docker-route

修复方案

docker 修复操作步骤：

1. 下载修复脚本，并上传到部署机 /data/kubewps 目录，/data 请以实际为准

2. 进入部署容器 kubewps，解压修复脚本

```
Plain Text

1 kubewps
2 unzip fix-docker-route.zip
```

3. 执行修复(必须是 kubewps 容器中且进入 fix-docker-route 目录)

用法 : fix_docker_route_07171550.sh < 部署用户名 > <fix|check|rollback>

部署用户名（即 kubewps.conf 中配置的用户）按实际填写，且需要 sudo 权限

```
Plain Text

1 cd fix-docker-route
2 bash fix_docker_route_07171550.sh  wps  fix  #注意wps替换为实际部署用户
```

4. 执行检查(必须是 kubewps 容器中且进入 fix-docker-route 目录)

```
Plain Text

1 bash fix_docker_route_07171550.sh wps check
```

验证：

访问域名 /open/v6/api/etcd/operate

访问域名 /open/api/etcd/operate

访问域名 /mgr/api/etcd/operate

访问域名 /mgr/api/mq/v1/receive/msg

访问域名 /open/api/tools/v1/collect/appactivity

访问域名 /mgr/api/tools/v1/collect/appactivity

访问域名 /open/api/deploy/operate

看下这些接口是不是 403（表示正常）

回退方案：

1. 回退命令(必须是 kubewps 容器中且进入 fix-docker-route 目录)

```
Plain Text
1 bash fix_docker_route_07171550.sh wps rollback
```

2. 执行检查(必须是 kubewps 容器中且进入 fix-docker-route 目录)

```
Plain Text
1 bash fix_docker_route_07171550.sh wps check
```