逐鹿云端之云原生安全攻防

王任飞

whoami

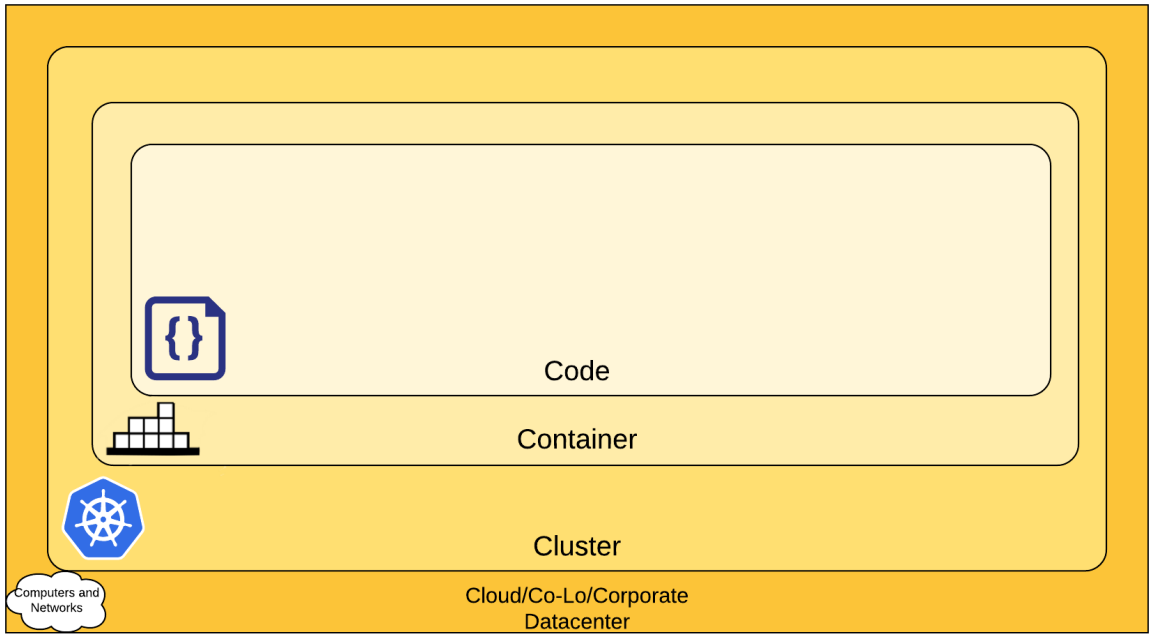
- 王任飞 (avfisher)
- 公众号“安全小飞侠”作者
- 某企业蓝军负责人，蓝星安全群群友，主要专注于红蓝对抗、漏洞研究、渗透测试、威胁情报、安全架构、云安全等领域。

Agenda

- 什么是云原生安全
- 云原生安全攻防现状分析
- 典型云原生安全攻防案例
- 云原生安全攻防趋势展望

什么是云原生安全

Kubernetes: 云原生安全是由**Code**、**Container**、**Cluster**、以及**Cloud**四个方面的安全构成的。



https://kubernetes.io/docs/concepts/security/overview/

CNCF：云原生安全是**将安全性构建到云原生应用程序中**，确保安全贯穿整个应用程序的生命周期，**具备适应代码快速更新和基础设施高度短暂的特点**。

Cloud Native Security

Security

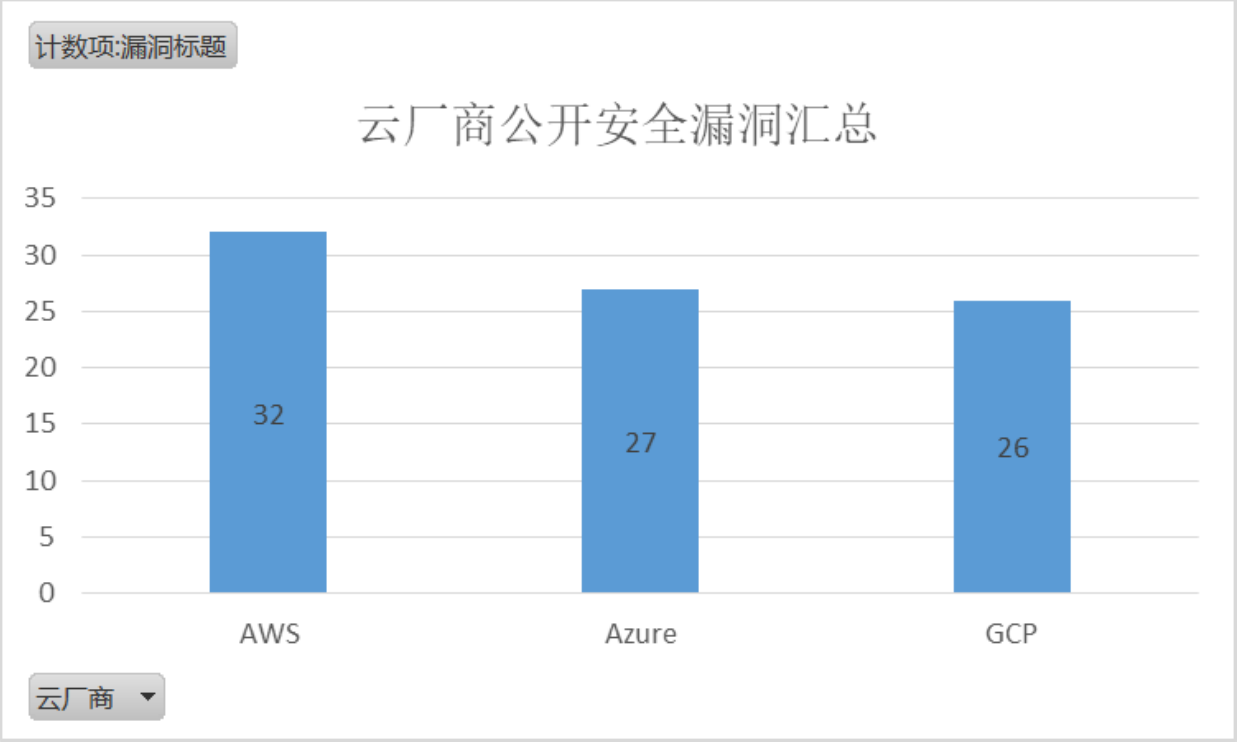
What it is

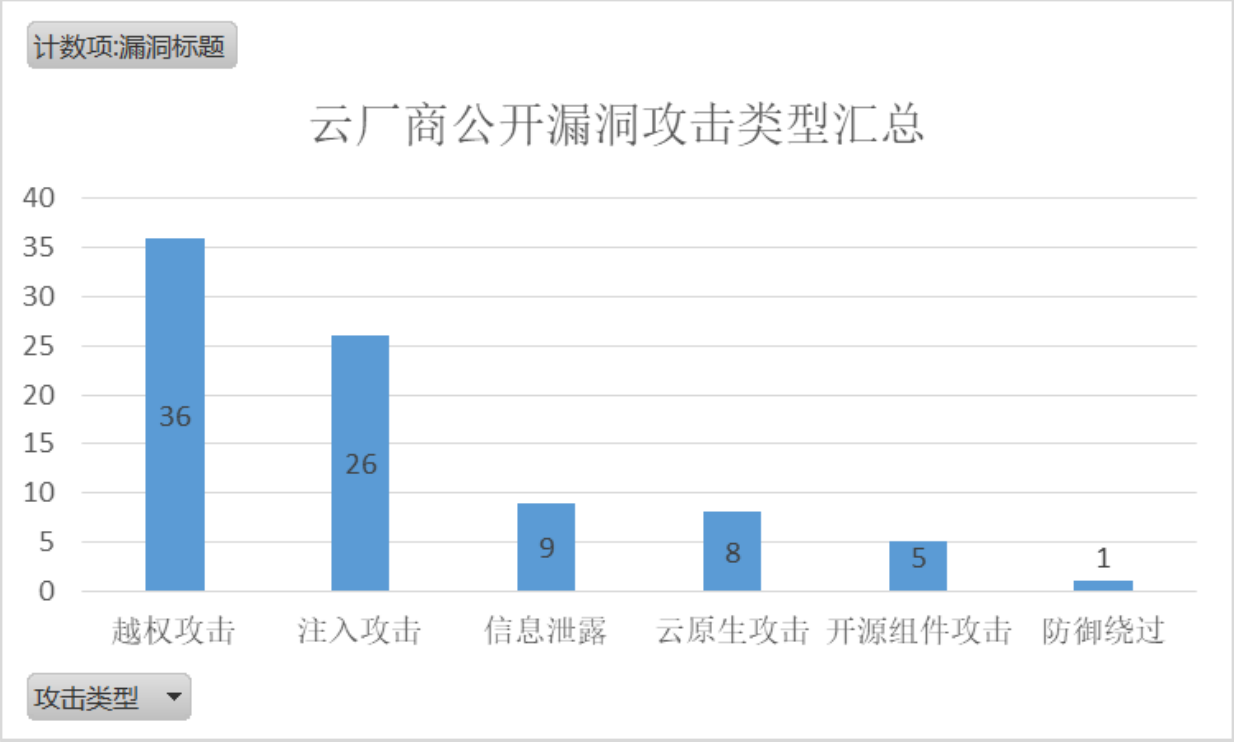
Cloud native security is an approach that builds security into **cloud native applications**. It ensures that security is part of the entire application lifecycle from development to production. Cloud native security seeks to ensure the same standards as traditional security models while adapting to the particulars of cloud native environments, namely rapid code changes and highly ephemeral infrastructure. Cloud native security is highly related to the practice called **DevSecOps**.

https://glossary.cncf.io/cloud-native-security/

云原生安全攻防现状分析

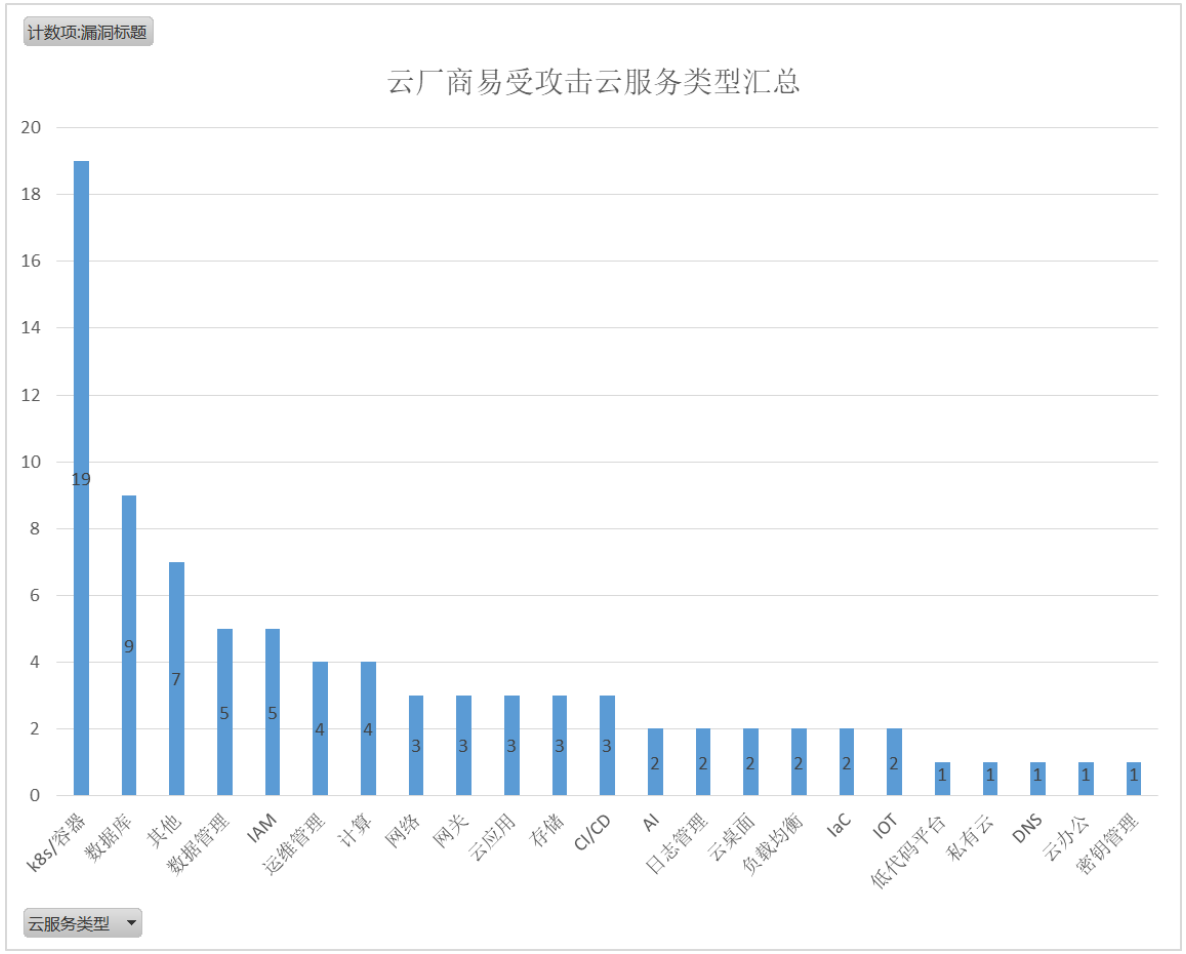
从云厂商公开的安全漏洞来看，TOP3云厂商均存在不少漏洞问题，其中主要的攻击类型包括：**越权攻击、注入攻击、信息泄露、云原生攻击、开源组件攻击**等。

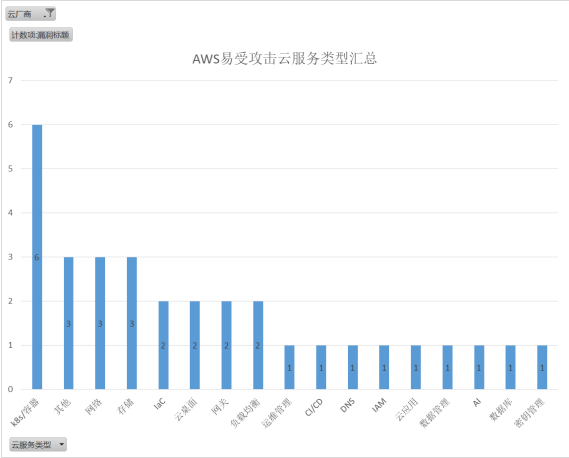


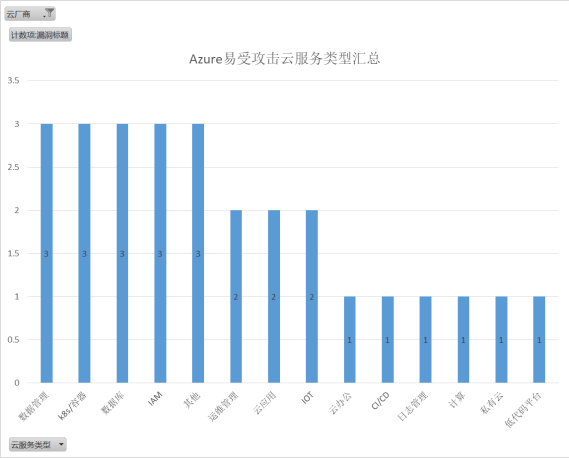


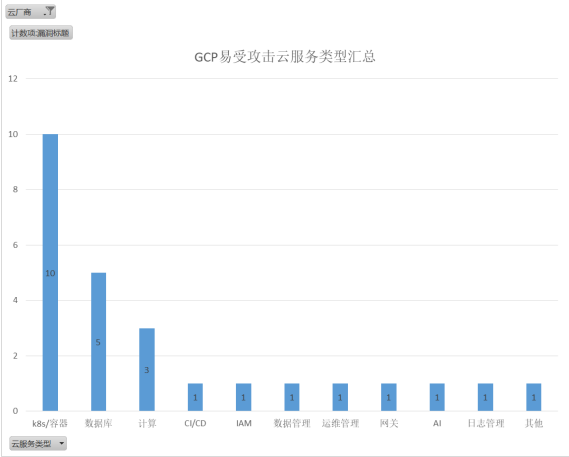
https://www.cloudvulndb.org/

云原生安全攻防现状分析



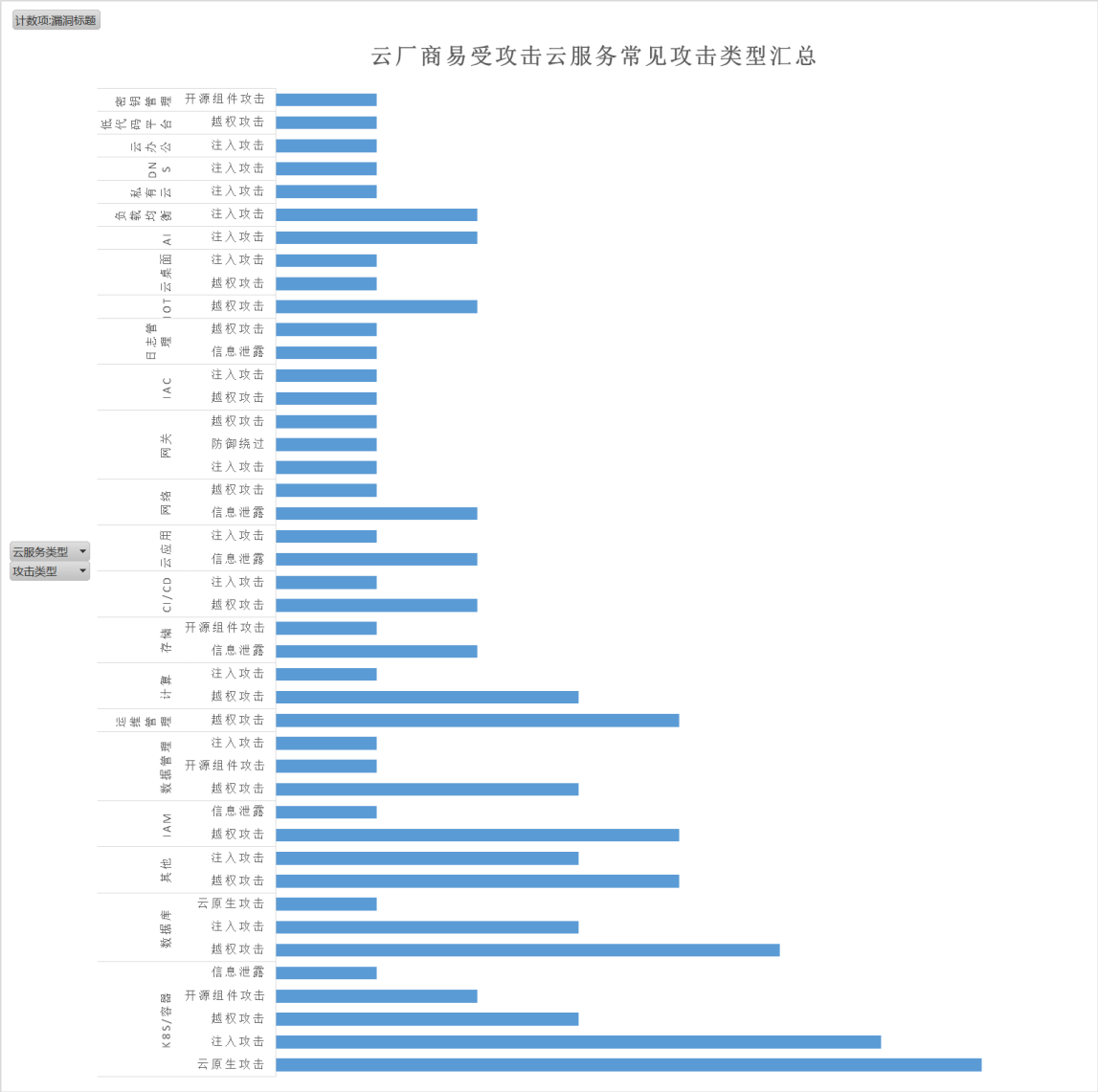






最易受攻击的云服务类型是：**k8s/容器、数据库、数据管理、IAM等**

云原生安全攻防现状分析



最易受攻击云服务的TOP攻击类型：

- k8s/容器：**云原生攻击、注入攻击**
- 数据库：**越权攻击、注入攻击**
- 数据管理：**越权攻击**
- IAM：**越权攻击**

典型云原生安全攻防案例

云服务类型： k8s/容器

攻击类型： 云原生攻击

攻击简介：

利用Google-managed Anthos Service Mesh的Istio控制面支持多集群部署通过新建恶意的GKE集群并部署Google-managed ASM导致RCE可直接访问Google-managed ASM底层VM实例的metadata

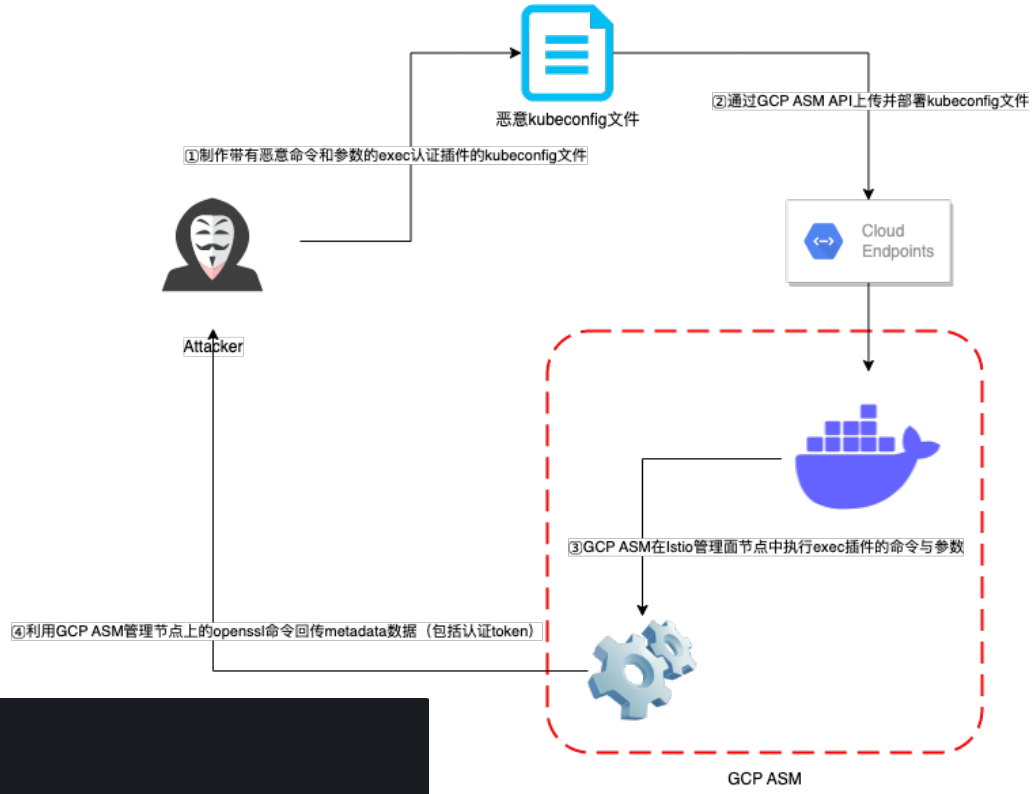
攻击过程：

① 制作带有恶意命令和参数的exec认证插件的kubeconfig文件

② 通过GCP ASM API上传并部署kubeconfig文件

③ GCP ASM在Istio管理面节点中执行exec插件的命令与参数

④ 利用GCP ASM管理节点上的openssl命令回传metadata数据（包括认证token）




```yaml
apiVersion: v1
kind: Config
current-context: default
clusters:
- name: default
  cluster:
    server: https://127.0.0.1
contexts:
- name: default
  context:
    cluster: default
    user: default
users:
- name: default
  user:
    exec:
      apiVersion: client.authentication.k8s.io/v1beta1
      command: /bin/sh
      args: ['-c', 'touch /tmp/flag']
```

https://lf.lc/vrp/203177829/

典型云原生安全攻防案例

云服务类型： k8s/容器

攻击类型： 注入攻击

攻击简介：

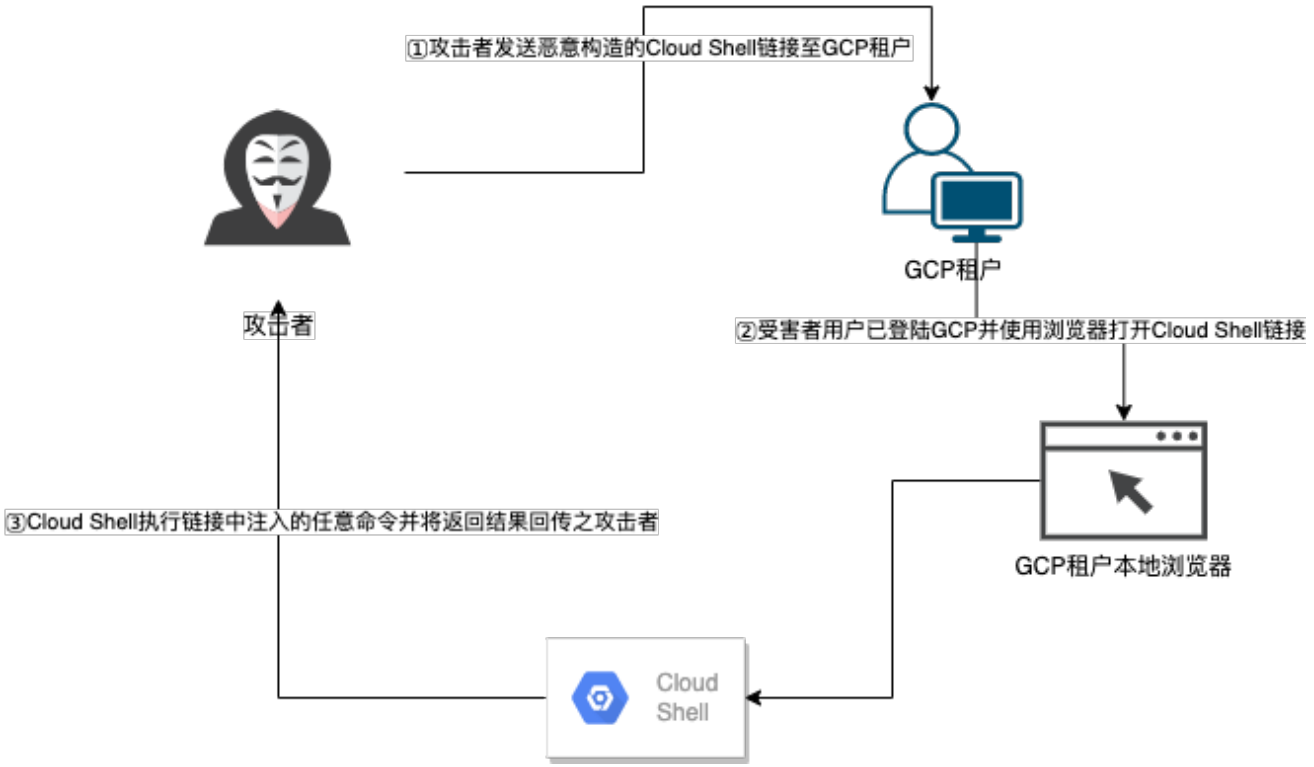
利用Google Cloud Shell校验逻辑不当借助Theia IDE实现Cloud Shell命令注入可绕过安全校验直接访问Cloud Shell底层VM实例的metadata

攻击过程：

① 攻击者发送恶意构造的cloudshell链接至GCP租户

② 受害者用户已登陆GCP并使用浏览器打开Cloud Shell链接

③ Cloud Shell服务执行链接中注入的任意命令并将返回结果回传之攻击者



POC:
https://shell.cloud.google.com/?show=ide&go_get_repo=";curl 0/service-accounts/default/token;%23&git_repo=github.com/GoogleCloudPlatform/gsutil

```
Welcome to Cloud Shell! Type "help" to get started.
To set your Cloud Platform project in this session use "gcloud config set project [PROJECT_ID]"
nowasky_jr@cloudshell:~$ cloudshell_open --repo_url "https://github.com/GoogleCloudPlatform/gsutil" --go_get "";echo "Command Injection";#" --page "editor" --force_new_clone
2020/12/29 14:39:04 Cloning https://github.com/GoogleCloudPlatform/gsutil into /home/nowasky_jr/cloudshell_open/gsutil
Cloning into '/home/nowasky_jr/cloudshell_open/gsutil'...
remote: Enumerating objects: 22, done.
remote: Counting objects: 100% (22/22), done.
remote: Compressing objects: 100% (22/22), done.
remote: Total 18132 (delta 8), reused 0 (delta 0), pack-reused 18110
Receiving objects: 100% (18132/18132), 15.30 MiB | 16.97 MiB/s, done.
Resolving deltas: 100% (13088/13088), done.
Command Injection
nowasky_jr@cloudshell:~/cloudshell_open/gsutil$
```

https://docs.google.com/document/d/1-TTCS6fS6kvFUkoJmX4Udr-czQ79lSUVXiWsiAED_bs/edit

典型云原生安全攻防案例

云服务类型： 数据库

攻击类型： 越权攻击

攻击简介：

利用Azure PostgreSQL权限配置不当实现本地提权及通过数据库备份功能证书校验逻辑不严实现跨账号数据库认证绕过

攻击过程：

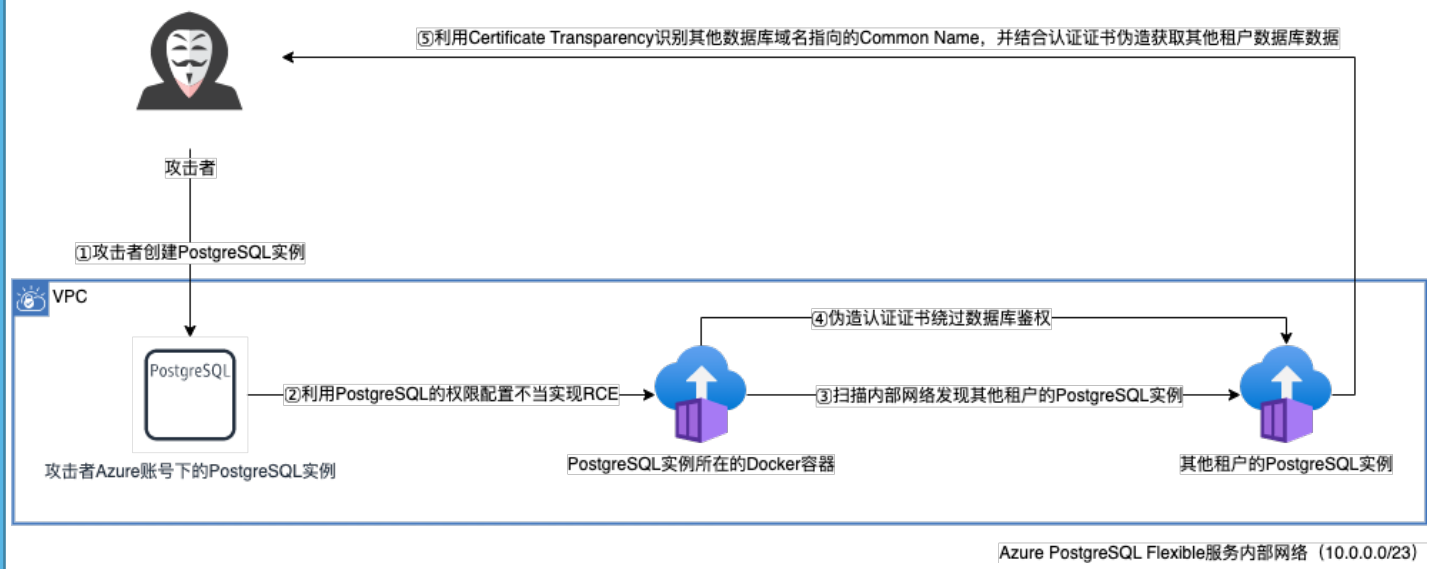
① 攻击者创建PostgreSQL实例

② 利用PostgreSQL的权限配置不当实现RCE

③ 扫描内部网络发现其他租户的PostgreSQL实例

④ 伪造认证证书绕过数据库鉴权

⑤ 利用Certificate Transparency识别其他数据库域名指向的Common Name，并结合认证证书伪造获取其他租户的PostgreSQL数据库数据



https://www.wiz.io/blog/wiz-research-discovers-extrareplica-cross-account-database-vulnerability-in-azure-postgresql/

典型云原生安全攻防案例

云服务类型： 数据库

攻击类型： 注入攻击

攻击简介：

利用AWS PostgreSQL的log_fdw扩展的路径穿越漏洞实现任意本地文件读取泄露RDS服务的内部认证凭据

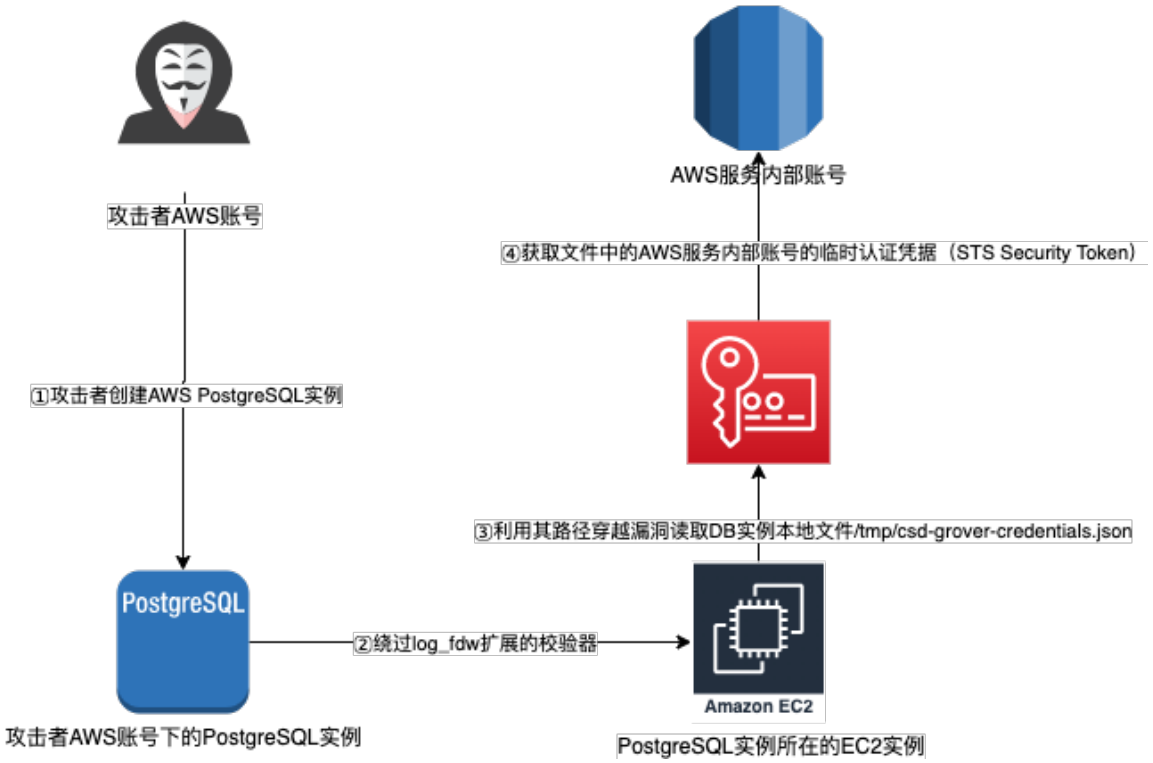
攻击过程：

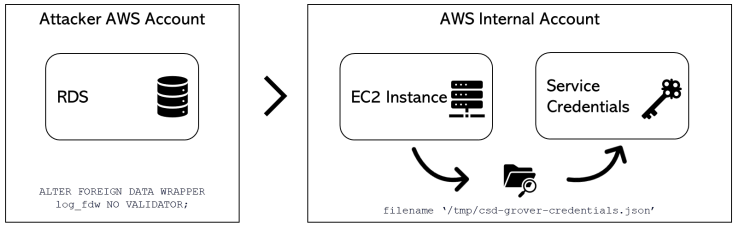
① 攻击者创建AWS PostgreSQL实例

② 绕过log_fdw扩展的校验器

③ 利用其路径穿越漏洞读取DB实例本地文件/tmp/csd-grover-credentials.json

④ 获取文件中的AWS服务内部账号的临时认证凭据（STS Security Token）





https://blog.lightspin.io/aws-rds-critical-security-vulnerability

典型云原生安全攻防案例

云服务类型：数据管理

攻击类型：越权攻击

攻击简介：

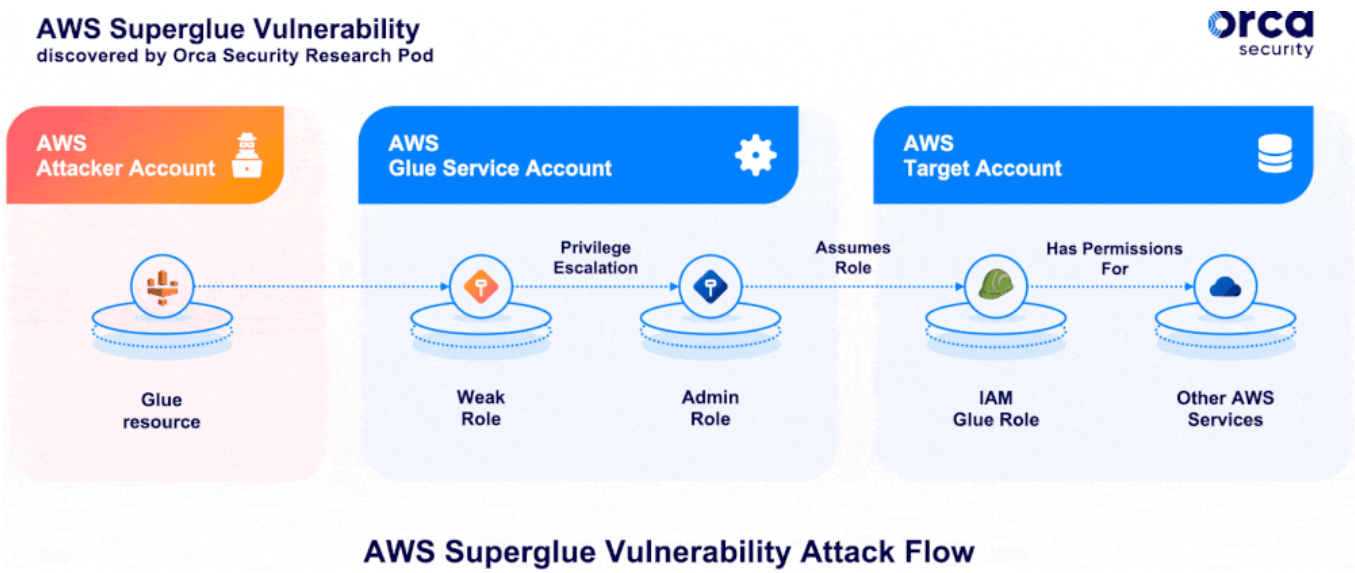
利用assume role提权至AWS Glue服务账号再结合其内部API的不安全配置获得其他使用了Glue服务的租户账号权限

攻击过程：

① 攻击者利用AWS Glue服务的一个正常功能获取Glue服务内部账号低权限角色的认证凭据

② 利用Glue服务内部API的不安全配置从低权限角色提权到管理员角色

③ 利用Glue服务内部账号的管理员角色通过角色委托（assume role）获得其他使用了Glue服务的租户账号权限



https://orca.security/resources/blog/aws-glue-vulnerability/

典型云原生安全攻防案例

云服务类型： IAM

攻击类型： 越权攻击

攻击简介：

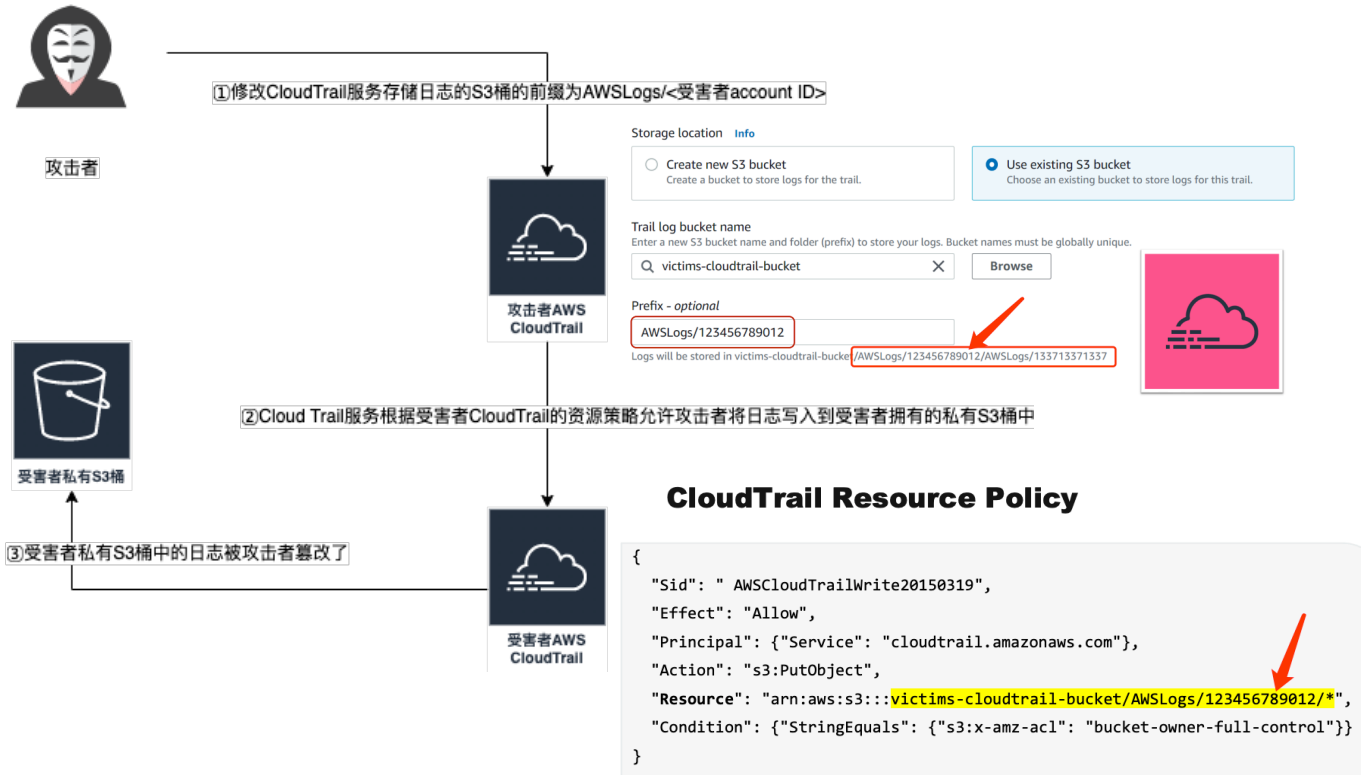
利用云服务的跨账号默认IAM权限配置不当，实现跨租户资源篡改

攻击过程：

① 攻击者在自身账号下修改CloudTrail服务存储日志的S3桶的前缀为AWSLogs/<受害者account ID>

② Cloud Trail服务根据受害者CloudTrail的默认资源策略允许攻击者将日志写入到受害者拥有的私有S3桶中

③ 受害者私有S3桶中的日志被攻击者篡改了



https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Breaking-The-Isolation-Cross-Account-AWS-Vulnerabilities.pdf

云原生安全攻防趋势展望

突破权限隔离

① IAM账号：AWS Landing Zone
② IAM策略：ABAC
③ 委托代理
④ 联邦认证：AWS STS security tokens、SAML

突破网络隔离

①传统的网络隔离边界：防火墙、路由器、交换机、VPN
②VPC：peering、endpoint、traffic mirror
③云专线：混合云、多云网络
④安全组

突破架构隔离

①物理多租：单租户独享
②逻辑多租：多租户共享

突破资源隔离

①虚拟机逃逸
②容器逃逸
③物理机CPU/芯片侧信道攻击

感谢观看