云厂商	漏洞标题	攻击类型	威胁分类（STRIDE）	受影响云服务	云服务类型	云架构元素类型	相关链接
AWS	利用AWS的ECS服务的Task Definition新建容器并通过EC2的metadata API获取临时AK/SK提权	云原生攻击	提权	ECS	k8s/容器	资源负载	https://rhinosecuritylabs.com/aws/pillaging-ecs-task-definitions-two-new-pacu-modules/
AWS	通过AWS ECS Task Definition可以获取敏感信息（Task Definition类似于k8s的kubeconfig文件）	云原生攻击	信息泄露	ECS	k8s/容器	资源负载	https://rhinosecuritylabs.com/aws/weaponizing-ecs-task-definitions-steal-credentials-running-containers/
AWS	利用AWS API Gateway服务可以绕过IP黑名单的限制	防御绕过	仿冒	APIG	网关	服务功能	https://rhinosecuritylabs.com/aws/bypassing-ip-based-blocking-aws/
AWS	滥用AWS VPC服务的TrafficMirror特性获取东西向流量中的敏感信息	信息泄露	信息泄露	VPC	网络	网络连接	https://rhinosecuritylabs.com/aws/abusing-vpc-traffic-mirroring-in-aws/
AWS	利用XXE读取本地文件和SSRF获取metadata	注入攻击	仿冒	CloudFormation	IaC	资源负载	https://orca.security/resources/blog/aws-cloudformation-vulnerability/
AWS	利用assume role提权至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	越权攻击	提权	Glue	数据管理	权限配置	https://orca.security/resources/blog/aws-glue-vulnerability/
AWS	S3漏洞利用（计算资源中列权限、过度依赖IAM防止数据泄露、非公开的桶中包含公开的存储对象）	信息泄露	信息泄露	S3	存储	权限配置	https://cloudsecurityalliance.org/blog/2020/06/18/3-big-amazon-s3-vulnerabilities-you-may-be-missing/
AWS	WorkSpaces（利用第三方软件SDK漏洞）	越权攻击	提权	WorkSpaces	云桌面	资源负载	https://www.sentinelone.com/labs/usb-over-ethernet-multiple-privilege-escalation-vulnerabilities-in-aws-and-other-major-cloud-services/
AWS	利用CNAME进行子域名接管	注入攻击	篡改	Route53	DNS	权限配置	https://0xpatrik.com/subdomain-takeover-ns/
AWS	利用云服务的跨账号默认IAM权限配置不当，如允许修改资源arn，实现跨租户资源获取）	越权攻击	提权	IAM	IAM	权限配置	https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Breaking-The-Isolation-Cross-Account-AWS-Vulnerabilities.pdf
AWS	AWS SageMaker Jupyter Notebook Instance Takeover（利用XSS->CSRF->安全恶意扩展->访问Metadata->获取AWS认证token）	注入攻击	仿冒	SageMaker	AI	服务功能	https://blog.lightspin.io/aws-sagemaker-notebook-takeover-vulnerability
AWS	CVE-2020-8897 SSRF Vulnerability in AWS KMS and Encryption SDK	开源组件攻击	仿冒	KMS	密钥管理	资源负载	https://github.com/google/security-research/security/advisories/GHSA-wggp-vphw-hphf
AWS	AWS: In-band key negotiation issue in the AWS S3 Crypto SDK for golang (CVE-2020-8912 and CVE-2020-8911)	开源组件攻击	仿冒	S3	存储	资源负载	https://github.com/google/security-research/security/advisories/GHSA-7f33-f4f5-xwgw
AWS	通过条件竞争修改AWS amazon-ssm-agent任意用户写的sudoers文件实现本地提权（CVE-2022-29527）	越权攻击	提权	SSM	运维管理	权限配置	https://bugzilla.suse.com/show_bug.cgi?id=1196556
AWS	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	注入攻击	信息泄露	RDS	数据库	部署架构	https://blog.lightspin.io/aws-rds-critical-security-vulnerability
AWS	AWS CloudShell Terminal（Cloud9）命令注入漏洞（CVE-2019-0542）	开源组件攻击	篡改	CloudShell	k8s/容器	资源负载	https://bugs.chromium.org/p/project-zero/issues/detail?id=2154
AWS	AWS: Launching EC2s did not require specifying AMI owner: CVE-2018-15869	注入攻击	仿冒	CLI	其他	服务功能	https://github.com/hashicorp/packer/issues/6584
AWS	AWS: ALB HTTP request smuggling	注入攻击	仿冒	ALB	负载均衡	部署架构	https://twitter.com/arkadiyt/status/1180174359840862209
AWS	利用具有CAP_NET_RAW Linux capability和hostNetwork=true的容器通过中间人劫持K8S集群的云宿主机node节点上的Metadata服务实现本地提权或者容器逃逸	云原生攻击	篡改	EKS	k8s/容器	资源负载	https://blog.champtar.fr/Metadata_MITM_root_EKS_GKE/
AWS	AWS: Execution in CloudFormation service account	越权攻击	提权	CloudFormation	IaC	权限配置	https://onecloudplease.com/blog/security-september-cataclysms-in-the-cloud-formations
AWS	AWS: Lightsail object storage access keys logged	信息泄露	信息泄露	Lightsail	云应用	应用数据	https://summitroute.com/blog/2021/08/05/lightsail_object_storage_concerns-part_1/
AWS	AWS API Gateway HTTP header smuggling	注入攻击	仿冒	APIG	网关	部署架构	https://www.intruder.io/research/practical-http-header-smuggling
AWS	aws-iam-authenticator AccessKeyID validation bypass (CVE-2022-2385)	越权攻击	提权	EKS	k8s/容器	权限配置	https://blog.lightspin.io/exploiting-eks-authentication-vulnerability-in-aws-iam-authenticator
AWS	Partial Path Traversal in com.amazonaws:aws-java-sdk-s3 (CVE-2022-31159)	信息泄露	信息泄露	S3	存储	资源负载	https://github.com/aws/aws-sdk-java/security/advisories/GHSA-c28r-hw5m-5gv3
AWS	ELB Cache mechanism HTTP header smuggling	注入攻击	篡改	ELB	负载均衡	部署架构	https://www.cloudvulndb.org/elb-cache-http-smuggling
AWS	Kubernetes: Multiple issues in aws-iam-authenticator	注入攻击	仿冒	EKS	k8s/容器	部署架构	https://bugs.chromium.org/p/project-zero/issues/detail?id=2066
AWS	IAM privilege escalation via undocumented CodeStar API	越权攻击	提权	CodeStar	CI/CD	权限配置	https://rhinosecuritylabs.com/aws/escalating-aws-iam-privileges-undocumented-codestar-api/
GCP	利用GCP CloudBuild服务的Service Account账号的token（metatdata API中获取）实现IAM的提权，即利用云服务的默认过多的IAM权限实现IAM的低权限提升	越权攻击	提权	CloudBuild	CI/CD	权限配置	https://rhinosecuritylabs.com/gcp/iam-privilege-escalation-gcp-cloudbuild/
GCP	利用GCP的各种服务特性实现IAM权限提升，即间接提权方式	越权攻击	提权	IAM	IAM	权限配置	https://github.com/RhinoSecurityLabs/GCP-IAM-Privilege-Escalation
GCP	利用k8s TLS Bootstapping机制进行提权	云原生攻击	提权	GKE	k8s/容器	资源负载	https://rhinosecuritylabs.com/cloud-security/kubelet-tls-bootstrap-privilege-escalation/
GCP	通过DHCP泛洪接管VM和获取ROOT访问权限	注入攻击	篡改	GCE	计算	网络连接	https://github.com/irsl/gcp-dhcp-takeover-code-exec
GCP	Privilege Escalation in Google Cloud Platform's OS Login	越权攻击	提权	OS Login	计算	权限配置	https://gitlab.com/gitlab-com/gl-security/security-operations/gl-redteam/red-team-tech-notes/-/tree/master/oslogin-privesc-june-2020
GCP	Google Cloud Platform (GCP) Service Account-based Privilege Escalation paths	越权攻击	提权	GCE, GCD	计算	权限配置	https://www.praetorian.com/blog/google-cloud-platform-gcp-service-account-based-privilege-escalation-paths/
GCP	GCP Default compute account is project Editor	越权攻击	提权	Resource Manager	运维管理	权限配置	https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts#disable_service_account_default_grants
GCP	GCP: AI Hub Jupyter Notebook instance CSRF	注入攻击	仿冒	Cloud AI HUB	AI	服务功能	https://blog.s1r1us.ninja/research/cookie-tossing-to-rce-on-google-cloud-jupyter-notebooks
GCP	利用具有CAP_NET_RAW Linux capability和hostNetwork=true的容器通过中间人劫持K8S集群的云宿主机node节点上的Metadata服务实现本地提权或者容器逃逸	云原生攻击	篡改	GKE	k8s/容器	资源负载	https://blog.champtar.fr/Metadata_MITM_root_EKS_GKE/
GCP	GCP: Exfiltrate data via the logs of GCP Org policy	信息泄露	信息泄露	Cloud Logging	日志管理	应用数据	https://trustoncloud.com/exfiltrate-data-from-your-super-secure-google-cloud-project-using-the-security-control-built-to-prevent-it/
GCP	Bypassing Identity-Aware Proxy	越权攻击	仿冒	IAP	网关	权限配置	https://www.seblu.de/2021/12/iap-bypass.html
GCP	Dataflow服务的JMX RMI端口未授权访问导致RCE并借助使用host网络的容器可直接访问GCE的metadata	开源组件攻击	仿冒	Dataflow	数据管理	资源负载	https://mbrancato.github.io/2021/12/28/rce-dataflow.html
GCP	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	云原生攻击	仿冒	Anthos Service Mesh (ASM)	k8s/容器	资源负载	https://lf.lc/vrp/203177829/
GCP	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	注入攻击	仿冒	Cloud Shell	k8s/容器	资源负载	https://docs.google.com/document/d/1-TTCS6fS6kvFUkoJmX4Udr-czQ79lSUVXiWsiAED_bs/edit
GCP	Postgres 服务帐户可以访问其他 RDS（MySQL、SQL Server 等）的 Docker 映像	云原生攻击	信息泄露	Cloud SQL	数据库	部署架构	https://irsl.medium.com/the-speckle-umbrella-story-part-2-fcc0193614ea
GCP	MySQL LOAD DATA LOCAL滥用导致MySQL连接客户端任意文件读取	注入攻击	信息泄露	Cloud SQL	数据库	资源负载	https://irsl.medium.com/the-speckle-umbrella-story-part-2-fcc0193614ea
GCP	利用Cloud SQL Auth Proxy的TLS1.2明文传输client certificates问题通过中间人攻击窃取IAM token、数据库凭据等	注入攻击	信息泄露	Cloud SQL	数据库	应用数据	https://irsl.medium.com/the-speckle-umbrella-story-part-2-fcc0193614ea
GCP	Cloud SQL Proxy信息泄露漏洞（项目和实例名称）	越权攻击	信息泄露	Cloud SQL	数据库	应用数据	https://irsl.medium.com/the-speckle-umbrella-story-part-2-fcc0193614ea
GCP	GCP Cloudshell Vulnerabilities: Escaping the Cloud Shell container	云原生攻击	提权	Cloud Shell	k8s/容器	资源负载	https://offensi.com/2019/12/16/4-google-cloud-shell-bugs-explained-introduction/
GCP	GCP Cloudshell Vulnerabilities: Python Language Server	注入攻击	篡改	Cloud Shell	k8s/容器	资源负载	https://offensi.com/2019/12/16/4-google-cloud-shell-bugs-explained-bug-1/
GCP	GCP Cloudshell Vulnerabilities: A custom Cloud Shell image	云原生攻击	提权	Cloud Shell	k8s/容器	资源负载	https://offensi.com/2019/12/16/4-google-cloud-shell-bugs-explained-bug-2/
GCP	GCP Cloudshell Vulnerabilities: Git clone	注入攻击	篡改	Cloud Shell	k8s/容器	资源负载	https://offensi.com/2019/12/16/4-google-cloud-shell-bugs-explained-bug-3/
GCP	GCP Cloudshell Vulnerabilities: Go and get pwned (CVE-2019-3902)	注入攻击	篡改	Cloud Shell	k8s/容器	资源负载	https://offensi.com/2019/12/16/4-google-cloud-shell-bugs-explained-bug-4/
GCP	Google Cloud Shell - Command Injection	注入攻击	篡改	Cloud Shell	k8s/容器	资源负载	https://bugra.ninja/posts/cloudshell-command-injection/
GCP	Cloud SQL escape to host	越权攻击	提权	Cloud SQL	数据库	资源负载	https://www.wiz.io/blog/the-cloud-has-an-isolation-problem-postgresql-vulnerabilities
Azure	GoldenSAML攻击主要针对联邦认证机制中使用的SAML Response的伪造	越权攻击	仿冒	ADFS	IAM	权限配置	https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps
Azure	Azure Container Instances (ACI)服务跨账号容器接管	云原生攻击	提权	ACI	k8s/容器	资源负载	https://unit42.paloaltonetworks.com/azure-container-instances/
Azure	NotLegit: Azure App Service vulnerability exposed hundreds of source code repositories	信息泄露	信息泄露	Azure App Service	云应用	服务功能	https://www.wiz.io/blog/azure-app-service-source-code-leak/
Azure	ChaosDB explained: Azure's Cosmos DB vulnerability walkthrough	越权攻击	提权	Azure Cosmos DB	数据库	部署架构	https://www.wiz.io/blog/chaosdb-explained-azures-cosmos-db-vulnerability-walkthrough/
Azure	OMIGOD - Azure OMI Management Interface Authentication Bypass (CVE-2021-38647)	越权攻击	提权	Azure OMI	其他	权限配置	https://blog.wiz.io/update-everything-you-need-to-know-about-omigod-from-the-team-that-discovered-it/
Azure	CredManifest: App Registration Certificates Stored in Azure Active Directory (CVE-2021-42306)	信息泄露	信息泄露	AAD	IAM	应用数据	https://www.netspi.com/blog/technical/cloud-penetration-testing/azure-cloud-vulnerability-credmanifest/
Azure	Remote Cloud Execution – Critical Vulnerabilities in Azure Cloud Infrastructure (Part I)	注入攻击	篡改	Azure Stack	私有云	权限配置	https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-i/
Azure	Remote Cloud Execution – Critical Vulnerabilities in Azure Cloud Infrastructure (Part II)	注入攻击	篡改	Azure App Service	云应用	资源负载	https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-ii/
Azure	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	越权攻击	提权	Azure Database for PostgreSQL	数据库	部署架构	https://www.wiz.io/blog/wiz-research-discovers-extrareplica-cross-account-database-vulnerability-in-azure-postgresql/
Azure	Azure Synapse pipelines and Azure Data Factory默认使用的第三方适配Amazon Redshift的ODBC连接器驱动存在命令注入漏洞（CVE-2022-29972）导致RCE可获取Azure服务敏感信息和跨租户数据	注入攻击	篡改	Azure Synapse Analytics, Azure Data Factory	数据管理	资源负载	https://orca.security/resources/blog/synlapse-critical-azure-synapse-analytics-service-vulnerability/
Azure	Azure: Cloudshell terminal escape (CVE-2019-0542)	开源组件攻击	篡改	CloudShell	k8s/容器	服务功能	https://twitter.com/_fel1x/status/1083085715565621250
Azure	Escalating Azure Privileges with the Log Analytics Contributor Role	越权攻击	提权	Log Analytics	日志管理	权限配置	https://www.netspi.com/blog/technical/cloud-penetration-testing/escalating-azure-privileges-with-the-log-analystics-contributor-role/
Azure	AutoWarp: Critical Cross-Account Vulnerability in Microsoft Azure Automation Service	越权攻击	提权	Azure Automation Service	运维管理	权限配置	https://orca.security/resources/blog/autowarp-microsoft-azure-automation-service-vulnerability/
Azure	Azure Service Fabric Container Elevation of Privilege Vulnerability (CVE-2022-30137)	越权攻击	提权	Azure Service Fabric	k8s/容器	资源负载	https://unit42.paloaltonetworks.com/fabricscape-cve-2022-30137/
Azure	Azure AD information disclosure via undocumented Diagnostics APIs	越权攻击	信息泄露	AAD	IAM	权限配置	https://www.secureworks.com/research/azure-active-directory-exposes-internal-information
Azure	Public admin access to Azure's Red Hat Update Infrastructure	越权攻击	篡改	Azure Red Hat Update Appliance	计算	权限配置	https://ianduffy.ie/2016/11/26/azure-bug-bounty-pwning-red-hat-enterprise-linux/
Azure	Escalating from Logic App Contributor to Root Owner in Azure	越权攻击	提权	Azure Logic Apps	低代码平台	权限配置	https://www.netspi.com/blog/technical/cloud-penetration-testing/azure-logic-app-contributor-escalation-to-root-owner/
Azure	在Azure Synapse Spark功能中利用filesharemount.sh脚本的条件竞争问题对任意文件执行chown操作从而实现本地提权	越权攻击	提权	Azure Synapse Analytics	数据管理	资源负载	https://orca.security/resources/blog/synapse-local-privilege-escalation-vulnerability-spark/
Azure	Azure Synapse: Local Privilege Escalation Vulnerability	越权攻击	提权	Azure Synapse Analytics	数据管理	资源负载	https://medium.com/tenable-techblog/microsoft-azure-synapse-pwnalytics-87c99c036291
Azure	利用CSTI和存储型XSS获得Azure Service Fabric Explorer服务的用户管理员权限（CVE-2022-35829）	注入攻击	提权	Azure Service Fabric Explorer	CI/CD	服务功能	https://orca.security/resources/blog/fabrixss-vulnerability-azure-fabric-explorer/
Azure	Azure Cosmos DB Notebook的forwardingId存在越权问题可导致RCE漏洞（CosMiss）	越权攻击	提权	Azure Cosmos DB	数据库	权限配置	https://orca.security/resources/blog/cosmiss-vulnerability-azure-cosmos-db/
AWS	利用AWS AppSync服务的confused deputy问题实现跨租户资源访问	越权攻击	提权	AppSync	数据管理	权限配置	https://securitylabs.datadoghq.com/articles/appsync-vulnerability-disclosure/
Azure	利用悬空子域名接管其他租户的Azure DevOps服务的账号	注入攻击	仿冒	Azure DevOps	CI/CD	权限配置	https://www.binarysecurity.no/posts/2022/11/azure-devops-takeover
IBM	PostgreSQL服务因不安全凭据管理可造成跨租户数据库的未授权访问	云原生攻击	提权	IBM Cloud Database for PostgreSQL	数据库	权限配置	https://www.wiz.io/blog/hells-keychain-supply-chain-attack-in-ibm-cloud-databases-for-postgresql
AWS	利用AWS ECR Public服务的未公开API跨租户越权修改容器镜像	越权攻击	提权	ECR Public	k8s/容器	权限配置	https://blog.lightspin.io/aws-ecr-public-vulnerability
Azure	利用Azure Serverless Function容器中本地进程提权实现容器逃逸	云原生攻击	提权	Azure Function Apps	k8s/容器	资源负载	https://unit42.paloaltonetworks.com/azure-serverless-functions-security/
Azure	Azure Cognitive Search服务跨租户网络隔离绕过	越权攻击	提权	Azure Cognitive Search	数据管理	权限配置	https://www.mnemonic.io/resources/blog/acsessed-cross-tenant-network-bypass-in-azure-cognitive-search/
AWS	利用未公开的私有API绕过CloudTrail的日志记录	防御绕过	仿冒	CloudTrail	日志管理	服务功能	https://securitylabs.datadoghq.com/articles/iamadmin-cloudtrail-bypass/
GCP	通过SSH公钥注入获取GCE访问权限	注入攻击	篡改	GCE	计算	服务功能	https://blog.stazot.com/ssh-key-injection-google-cloud/
Azure	利用Kudo提供的SCM面板的CSRF攻击多个Azure Web服务	注入攻击	仿冒	Azure Function Apps, Azure App Service, Azure Logic Apps	云应用	服务功能	https://ermetic.com/blog/azure/emojideploy-smile-your-azure-web-service-just-got-rced/
Azure	通过commit message修改Azure DevOps流水线执行过程中的环境变量可导致软件供应链攻击	注入攻击	篡改	Azure DevOps	CI/CD	服务功能	https://www.legitsecurity.com/blog/remote-code-execution-vulnerability-in-azure-pipelines-can-lead-to-software-supply-chain-attack
Aliyun	阿里云PostgreSQL服务因不安全配置导致容器逃逸可造成跨租户数据库的未授权访问	云原生攻击	提权	ApsaraDB RDS for PostgreSQL, AnalyticDB for PostgreSQL	数据库	部署架构	https://www.wiz.io/blog/brokensesame-accidental-write-permissions-to-private-registry-allowed-potential-r