

云原生安全威胁分析与 能力建设白皮书

中国联通研究院

中国联通网络安全研究院

下一代互联网宽带业务应用国家工程研究中心

2023年11月

版权声明

本报告版权属于中国联合网络通信有限公司研究院，并受法律保护。转载、摘编或利用其他方式使用本报告文字或者观点的，应注明“来源：中国联通研究院”。违反上述声明者，本院将追究其相关法律责任。



中国联通研究院

目 录

| | |
|--------------------------|----|
| 一、云原生安全概述 | 9 |
| 1.1 云原生及云原生安全 | 9 |
| 1.1.1 云原生 | 10 |
| 1.1.2 云原生安全 | 12 |
| 1.2 云原生安全发展 | 14 |
| 1.3 云原生安全风险 | 17 |
| 二、云原生关键技术威胁全景 | 19 |
| 2.1 云原生安全威胁分析 | 19 |
| 2.2 路径 1：镜像攻击 | 21 |
| 2.2.1 镜像投毒攻击 | 21 |
| 2.2.2 镜像仓库攻击 | 22 |
| 2.2.3 中间人攻击 | 22 |
| 2.2.4 敏感信息泄露攻击 | 22 |
| 2.2.5 针对镜像不安全配置的攻击 | 22 |
| 2.3 路径 2：容器攻击 | 23 |
| 2.3.1 守护进程攻击 | 23 |
| 2.3.2 容器提权和逃逸攻击 | 24 |
| 2.3.3 拒绝服务攻击 | 25 |

| | |
|------------------------------|----|
| 2.3.4 容器网络攻击 | 26 |
| 2.4 路径 3：编排工具攻击 | 26 |
| 2.4.1 k8s 组件攻击 | 27 |
| 2.4.2 服务对外暴露攻击 | 27 |
| 2.4.3 业务 pod 攻击 | 28 |
| 2.4.4 集群环境下的横向攻击 | 29 |
| 2.4.5 k8s 管理平台攻击 | 29 |
| 2.4.6 第三方组件攻击 | 29 |
| 2.5 路径 4：微服务攻击 | 29 |
| 2.5.1 API 攻击 | 30 |
| 2.5.2 API 网关攻击 | 32 |
| 2.5.3 微服务应用攻击 | 32 |
| 2.6 路径 5：Serverless 攻击 | 33 |
| 2.6.1 事件注入攻击 | 34 |
| 2.6.2 敏感数据泄露攻击 | 34 |
| 2.6.3 身份认证攻击 | 35 |
| 2.6.4 权限滥用攻击 | 35 |
| 2.6.5 拒绝服务攻击 | 36 |

| | |
|-------------------------------------|----|
| 2.6.6 针对函数供应链的攻击 | 36 |
| 三、典型攻击场景分析 | 37 |
| 3.1 镜像投毒攻击 | 37 |
| 3.1.1 攻击场景介绍 | 37 |
| 3.1.2 攻击过程复现 | 38 |
| 3.2 挂载 Docker Socket 导致容器逃逸攻击 | 38 |
| 3.2.1 攻击场景介绍 | 38 |
| 3.2.2 攻击过程复现 | 39 |
| 3.3 k8s 权限提升攻击 | 40 |
| 3.3.1 攻击场景介绍 | 40 |
| 3.3.2 攻击过程复现 | 41 |
| 3.4 Istio 认证策略绕过攻击 | 43 |
| 3.4.1 攻击场景介绍 | 43 |
| 3.4.2 攻击过程复现 | 45 |
| 四、云原生应用保护能力建设 | 47 |
| 4.1 制品安全能力建设 | 47 |
| 4.1.1 代码安全 | 48 |
| 4.1.2 镜像安全 | 49 |

| | |
|----------------------------|----|
| 4.1.3 制品环境安全 | 50 |
| 4.1.4 安全检测 | 52 |
| 4.2 运行时安全能力建设 | 53 |
| 4.2.1 Web 应用和 API 安全 | 54 |
| 4.2.2 云原生运行时安全 | 56 |
| 4.2.3 网络微隔离 | 58 |
| 4.3 基础设施安全能力建设 | 59 |
| 4.3.1 基础设施即代码安全 | 59 |
| 4.3.2 权限管理 | 60 |
| 4.3.3 云原生安全态势 | 60 |
| 五、总结与展望 | 62 |
| 六、参考文献 | 64 |

