网络安全预警通报

2024 年第 6 期 （总第 49 期）

西安交通大学网络信息中心 2024 年 7 月 18 日

【预警类型】高危预警

【预警内容】

Nacos 远程代码执行漏洞分析、检测和加固防御通告

一、漏洞概述

Nacos 是一个更易于构建云原生应用的动态服务发现、配置管理和服务管理平台，支持多种开箱即用的以服务为中心的架构特性，无缝支持 Kubernetes 和 Spring Cloud，具备企业级 SLA 的开源产品．近期监测到了 Nacos 0day 相关信息，对此“0day”漏洞进行跟进分析。

二、漏洞详情

Nacos 是阿里巴巴开源的一个动态服务发现、配置管理和服务管理平台，它致力于帮助用户更轻松地构建基于微服务架构的云原生应用。Nacos 提供了服务发现和健康检查、动态配置服务、动态 DNS 服务以及服务和元数据管理等功能，通过支持 Dubbo、Spring Cloud 等主流微服务框架

和 Kubernetes 生态，Nacos 能有效提升系统的可用性、伸缩性和管理效率，帮助开发者简化复杂的分布式系统管理，并提升开发与运维的协作效率。

攻击者可通过 removal 接口使 Nacos 数据库加载恶意 JAR 包，之后通过 derby 接口在 Nacos 中执行任意 derby SQL 语句，进而执行任意系统命令。

注意事项：该漏洞在利用过程中访问的两个接口 /nacos/v1/cs/ops/data/removal 和 /nacos/v1/cs/ops/derby 均需要管理员权限才能访问，Nacos 部分版本默认配置未进行鉴权，导致此“0day”漏洞产生。

三、漏洞影响范围

Nacos<= v2.4.0 BETA, <= v2.3.2

截止 2024.7.16，最新测试版本 2.4.0、最新稳定版本 2.3.2 均受影响

四、漏洞缓解措施

1．开启鉴权

依据 Nacos 官方文档开启鉴权方法如下：

非 Docker 环境

通过 application.properties 配置文件开启鉴权。

开启鉴权之前，application.properties 中的配置信息为：

```
### If turn on auth system:
nacos.core.auth.enabled=false
```

开启鉴权之后，application.properties 中的配置信息为：

1. ### If turn on auth system:

2. nacos.core.auth.system.type=nacos

3. nacos.core.auth.enabled=true

Docker 环境

1）官方镜像

在启动 docker 容器时，添加如下环境变量

NACOS_AUTH_ENABLE=true

2）自定义镜像

自定义镜像，请在构建镜像之前，修改 nacos 工程中的 application.properties 文件。

将下面这一行配置信息：

1. nacos.core.auth.enabled=false

修改为：

1. nacos.core.auth.system.type=nacos

2. nacos.core.auth.enabled=true

然后再配置 nacos 启动命令。

2．设置强密码

将后台登录密码修改为强密码，该漏洞执行依赖于后台权限。

3．更新补丁

及时更新补丁，官网暂未发布补丁，可实时关注官网更新信息(https://nacos.io/download/nacos-server/)。