安全通告

关于 Alibaba Nacos derby 存在远程代码执行漏洞的预警通报

发布日期：2024-7-18

[2024]016 号

漏洞描述

2024 年 7 月 18 日通过监测发现，Alibaba Nacos derby 存在远程代码执行漏洞，该漏洞是由于 Alibaba Nacos 部分版本中 derby 数据库默认可以未授权访问，恶意攻击者利用此漏洞可以未授权执行 SQL 语句，从而远程加载恶意构造的 jar 包，最终导致任意代码执行。Nacos 是一个动态命名和配置服务的开源项目，旨在帮助用户构建云原生应用。它提供了动态服务发现、配置管理和服务共享等基础设施，适用于各种云环境，包括私有云、混合云和公有云。

漏洞危害

攻击者利用这一漏洞可以未授权执行 SQL 语句，从而远程加载恶意构造的 jar 包，最终导致任意代码执行。

漏洞等级

高危

受影响版本

Alibaba Nacos ≤ 2.4.0

修复方案

目前官方已经发布了解决此漏洞的相关补丁，建议受影响用户升级至安全版本。

https://nacos.io/download/nacos-server

参考链接

https://nacos.io/zh-cn/docs/v2/guide/user/auth.html