防火墙，IPS，LB是否涉及Nacosderby 接口SQL 注入导致RCE 漏洞

漏洞相关 **孔凡安** 4天前 发表

漏洞相关信息

漏洞编号： 暂无
漏洞名称： Nacosderby 接口SQL 注入导致RCE 漏洞
产品型号及版本： Comware V5/V7/V9

漏洞描述

一、漏洞概述
漏洞名称：Nacosderby 接口SQL 注入导致RCE 漏洞
漏洞等级：高危
漏洞描述：Nacos 是一个用于动态服务发现和配置以及服务管理的平台，Derby 是一个轻量级的嵌入式数据库。接口/nacos/v1/cs/ops/derby 和 /nacos/v1/cs/ops/data/removal 在使用Derby 数据库作为内置数据源时。用于运维人员进行数据运维和问题排查，在使用standalone 模式启动Nacos 时，为了避免因搭建外置数据库而占用额外的资源，会使用Derby 数据库作为数据源。受影响版本的Nacos 默认未开启身份认证，/data/removal 接口存在条件竞争漏洞，攻击者可借此接口执行恶意SQL，加载恶意jar 并注册函数，随后可以在未授权条件下利用derbysql 注入漏洞（CVE-2021-29442）调用恶意函数来执行恶意代码。此前官方开发者认为属于功能特性，未做处理，后在2.4.0 版本中通过增加derbyOpsEnabled 选项默认关闭derby 接口来避免被滥用。
二、影响范围
nacos 2.3.2
nacos 2.4.0
三、修复建议
1.将组件com.alibaba.nacos:nacos-config 升级至2.4.0 及以上版本
2.将组件nacos 升级至2.4.0 及以上版本

漏洞解决方案

防火墙，IPS，LB不没有使用相关漏洞组件，所以不涉及该漏洞。