# 0001

漏洞名称：Zookeeper未授权访问

漏洞时间：------

CVE编号：------

影响平台：zookeeper

影响范围：zookeeper

介绍：ZooKeeper默认开启在2181端口，在未进行任何访问控制情况下，攻击者可通过执行envi命令获得系统大量的敏感信息，包括系统名称、Java环境。

POC：echo envi | nc ip port

# 0002

漏洞名称：Apache ZooKeeper安全限制绕过漏洞

漏洞时间：2018-05-21

CVE编号：CVE-2018-8012

影响平台：windows、linux

影响版本：Apache Group ZooKeeper < 3.4.10

Apache Group ZooKeeper 3.5.0-alpha-3.5.3-beta

介绍：Apache Zookeeper是美国阿帕奇（Apache）软件基金会的一个软件项目，它能够为大型分布式计算提供开源的分布式配置服务、同步服务和命名注册等功能。 Apache ZooKeeper 3.4.10之前版本和3.5.0-alpha版本至3.5.3-beta版本中存在访问控制错误漏洞，该漏洞源于程序没有强制执行身份验证/授权检测。攻击者可利用该漏洞修改目标系统上的数据。

EXP：暂无