nacos突然爆出最新的RCE 0day，受影响版本如下：

受影响版本：nacos2.3.2nacos2.4.0

本次环境是在windows系统复现，因此需要访问下面的nacos官方地址去下载。

https://github.com/alibaba/nacos/releases/tag/2.3.2



点击下载并解压之后，进入nacos的 bin 目录下进行启动。

Windows下：startup.cmd -m standaloneLinux下：startup.sh -m standalone

默认启动端口为8848。



在浏览器上输入 http://127.0.0.1:8848/nacos

就会直接跳转到nacos的后台界面。



开始下载nacos rce poc

下载脚本https:*//github.com/ayoundzw/nacos-poc*

作者描述如下：

因为某些原因，公开一个nacos的0day环境准备：下载nacos2.3.2或2.4.0版本，解压，使用 startup.cmd -m standalone 启动nacos 补充POC信息 POC是一个python项目，依赖requests和flask，请先使用requiments.txt安装依赖 配置config.py中的ip和端口，执行service.py，POC攻击需要启动一个jar包下载的地方，jar包里可以放任意代码，都可执行，我这里放了一个接收参数执行java命令的 2.执行exploit.py，输入地址和命令即可执行。

下载后，里面什么内容都不需要修改。



先开启服务，服务的端口和ip在config.py中，不要造成端口冲突。



然后就是运行攻击脚本，设置目标url和使用的命令。



其他版本测试，也是能够成功。

