JBOOS反序列化漏洞复现

TimeS0ng / 2017-12-13 09:38:00 / 浏览数 3241 安全技术 技术讨论 顶(0) 踩(0)

0x00. 漏洞描述

2017年9月14日，国家信息安全漏洞共享平台（CNVD）收录了JBOSS Application Server反序列化命令执行漏洞（CNVD-2017-33724，对应CVE-2017-12149），远程攻击者利用漏洞可在未经任何身份验证的服务器主机上执行任意代码。漏

0x01. 漏洞复现

1). 环境准备

1. JBOSS下载地址：http://download.jboss.org/jbossas/6.1/jboss-as-distribution-6.1.0.Final.zip

2. EXP下载地址：https://github.com/yunxu1/jboss-_CVE-2017-12149

2). 环境搭建

第一步：下载JBOSS环境，并解压

```
wget http://download.jboss.org/jbossas/6.1/jboss-as-distribution-6.1.0.Final.zip
```

第二步：修改配置文件，使网络中的主机都能访问JBOSS

```
vim ~/jboss-6.1.0.Final/server/default/deploy/jbossweb.sar/server.xml
```

第三步：启动JBOSS

```
./jboss-6.1.0.Final/bin/run.sh
```

第四步：下载EXP

```
git clone https://github.com/yunxu1/jboss-_CVE-2017-12149
```

3). 信息收集

第一步：利用nmap对目标主机进行常用端口扫描

```
nmap 192.168.1.111 -A
```

第二步：访问目标主机的8080端口，看看能否正常访问

4). 漏洞利用

利用刚才下载好的EXP进行漏洞利用，打开jboss反序列化_CVE-2017-12149.jar

0x02. 总结

行千里路，不如读万卷书...

上一篇：HITCON 2017 Baby^... 下一篇：初探MITMF

1. 0 条回复
   - 动动手指，沙发就是你的了！

目录