河南省教育信息安全中心

Apache Tomcat Session 反序列化代码执行漏洞预警

2021 年 03 月 09 日

Apache Tomcat Session 反序列化代码执行漏洞

事件描述

近日，Apache 软件基金会发布安全通告，修复了一个通过会话持久性进行 RCE 的漏洞，此漏洞为 CVE-2020-9484 的补丁绕过，如果使用了 Tomcat 的 session 持久化功能，不安全的配置将导致攻击者可以发送恶意请求执行任意代码，成功利用此漏洞需要同时满足以下 4 个条件：

1）攻击者能够控制服务器上文件的内容和文件名称；

2）服务器 PersistenceManager 配置中使用了 FileStore；

3）PersistenceManager 中的 sessionAttributeValueClassNameFilter 被配置为“null”，或者过滤器不够严格，导致允许攻击者提供反序列化数据的对象；攻击者知道使用的 FileStore 存储位置到攻击者可控文件的相对路径。

影响范围

Apache Tomcat 10.0.0-M1—10.0.0

Apache Tomcat 9.0.0.M1—9.0.41

Apache Tomcat 8.5.0—8.5.61

Apache Tomcat 7.0.0—7.0.107

漏洞检测

1）从 Apache Tomcat 官网下载的安装包名称中会包含 Tomcat 的版本号，如果用户解压后没有更改 Tomcat 的目录名称，可以通过查看文件夹名称来确定当前使用的本。

如果解压后的 Tomcat 目录名称被修改过，或者通过 Windows Service Installer 方式安装，可使用软件自带的 version 模块来获取当前的版本。也可以进入 Tomcat 安装目录的 bin 目录，运行 version.bat（Linux 运行 version.sh）后，可查看当前的软件版本号。

```
D:\Program Files\Apache Software Foundation\Tomcat 9.0\bin>version.bat
Using CATALINA_BASE:   "D:\Program Files\Apache Software Foundation\Tomcat 9.0"
Using CATALINA_HOME:   "D:\Program Files\Apache Software Foundation\Tomcat 9.0"
Using CATALINA_TMPDIR: "D:\Program Files\Apache Software Foundation\Tomcat 9.0\t
emp"
Using JRE_HOME:        "D:\Program Files\Java\jdk1.8.0_131"
Using CLASSPATH:       "D:\Program Files\Apache Software Foundation\Tomcat 9.0\b
in\bootstrap.jar;D:\Program Files\Apache Software Foundation\Tomcat 9.0\bin\tomc
at-juli.jar"
Server version: Apache Tomcat/9.0.5
Server built:   Feb 6 2018 21:42:23 UTC
Server number:  9.0.5.0
OS Name:        Windows 7
OS Version:     6.1
Architecture:   amd64
JVM Version:    1.8.0_131-b11
JVM Vendor:     Oracle Corporation
D:\Program Files\Apache Software Foundation\Tomcat 9.0\bin>
```

2）查看 conf/context.xml 文件或具体项目的 server.xml 文件中，是否存在以下<Manager>节点。

```
context.xml
1
2  <Manager className="org.apache.catalina.session.PersistentManager" >
3      debug=0
4      saveOnRestart="true"
5      maxActiveSession="-1"
6      minIdleSwap="-1"
7      maxIdleSwap="-1"
8      maxIdleBackup="-1"
9      <Store className="org.apache.catalina.session.FileStore" directory="../session" />
10
11 //这里代表的是文件持久化.也可以自己实现Store
12 </Manager>
```

若当前版本在受影响范围内且在 PersistenceManager 配置中使用了 FileStore，则可能存在安全风险

处置建议

1）官方已经发布新版本修复该漏洞，详细信息如下：

Apache Tomcat 10.0.2：https://tomcat.apache.org/download-10.cgi

Apache Tomcat 9.0.43：https://tomcat.apache.org/download-90.cgi

Apache Tomcat 8.5.63：https://tomcat.apache.org/download-80.cgi

Apache Tomcat 7.0.108：https://tomcat.apache.org/download-70.cgi

2）若相关用户暂时无法进行升级操作，也可采用以下措施进行临时缓解：

禁止使用 Session 持久化功能 FileStore，或者单独配置 sessionAttributeValueClassNameFilte 的值来确保只有特定属性的对象可以被序列化与反序列化。

鉴于该漏洞影响范围较大，潜在危害程度较高，各单位要及时通知相关用户，核查 Apache Tomcat 使用情况，修补漏洞，消除安全隐患。