CVE-2017-12615 Tomcat远程代码执行漏洞复现

ly55521 / 2017-09-21 02:51:43 / 浏览数 5653 安全技术 漏洞分析 顶(0) 踩(0)

一. 漏洞简介

CVE-2017-12615 看没人发， 来发一个。

漏洞描述：Tomcat CVE-2017-12615远程代码执行漏洞 / CVE-2017-12616信息泄漏。
2017年9月19日，Apache
Tomcat官方确认并修复了两个高危漏洞，漏洞CVE编号:CVE-2017-12615和CVE-2017-12616,该漏洞受影响版本为7.0-7.80之间，在一定条件下，攻击者可以利用这两个漏
JSP 文件的源代码，或是通过精心构造的攻击请求，向用户服务器上传恶意JSP文件，通过上传的 JSP 文件
，可在用户服务器上执行任意代码，从而导致数据泄露或获取服务器权限，存在高安全风险。
CVE-2017-12616：信息泄露漏洞
当 Tomcat 中使用了 VirtualDirContext 时，攻击者将能通过发送精心构造的恶意请求，绕过设置的相关安全限制，或是获取到由 VirtualDirContext
提供支持资源的 JSP 源代码。
CVE-2017-12615：远程代码执行漏洞
当 Tomcat 运行在 Windows 主机上，且启用了 HTTP PUT 请求方法（例如，将 readonly 初始化参数由默认值设置为
false），攻击者将有可能可通过精心构造的攻击请求向服务器上传包含任意代码的 JSP 文件。之后，JSP 文件中的代码将能被服务器执行。
通过以上两个漏洞可在用户服务器上执行任意代码，从而导致数据泄露或获取服务器权限，存在高安全风险。

影响版本:
CVE-2017-12616影响范围：Apache Tomcat 7.0.0 - 7.0.80
CVE-2017-12615影响范围： Apache Tomcat 7.0.0 - 7.0.79

参考链接：
CVE-2017-12615：
https://tomcat.apache.org/security-7.html
http://tomcat.apache.org/securit ... pache_Tomcat_7.0.81

二. 利用条件
CVE-2017-12615漏洞利用需要在Windows环境，且需要将 readonly 初始化参数由默认值设置为 false，经过实际测试，Tomcat
7.x版本内web.xml配置文件内默认配置无readonly参数，需要手工添加，默认配置条件下不受此漏洞影响。
CVE-2017-12616漏洞需要在server.xml文件配置VirtualDirContext参数，经过实际测试，Tomcat
7.x版本内默认配置无VirtualDirContext参数，需要手工添加，默认配置条件下不受此漏洞影响。
根据绿盟最新研究在linux下也有影响，建议关闭PUT方法。

三. 漏洞测试
3.1白盒测试
开发人员检查是否使用受影响范围内的Apache Tomcat版本
3.2黑盒测试
1.首先搭建tomcat环境，需要预装下jdk，安装流程和配置参考：
http://www.ouyaoxiazai.com/soft/stgj/133/45254.html
搭建成功后，访问 http://10.74.53.11:8080/

2.开启PUT方法
安装好后，修改 C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\web.xml 配置文件，增加 readonly 设置为 false

3.然后使用burpsuite抓包把GET方法转为PUT方法写入数据，如下：

注意：PUT路径要用/结束，写入成功后，会返回201或者200，如果返回404说明没有写/，使用

写入成功后，在服务器的 web目录，如下
C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\ROOT增加了test.jsp文件

4.访问上传的木马 http://10.74.53.11:8080/test.jsp?pwd=023&i=whoami

复现参考：https://www.secfree.com/article-399.html
POC&EXP参考：
https://github.com/fupinglee/MyP ... mp;isappinstalled=1

四. 解决方案

根据业务评估配置readonly和VirtualDirContext值为Ture或注释参数，禁用PUT方法并重启tomcat，临时规避安全风险，升级为最新版本；
注意： 如果禁用PUT方法，对于依赖PUT方法的应用，可能导致业务失效。
官方已经发布Apache Tomcat 7.0.81 版本修复了两个漏洞建议升级最新版。

点击收藏 | 0 关注 | 0
上一篇：Tomcat信息泄漏和远程代码执行... 下一篇：Python沙箱逃逸的n种姿势

1. 3 条回复


hades 2017-09-22 01:48:30

辛苦

0 回复Ta


酷帥王子 2017-09-22 02:01:16

我在某论坛找到一个python利用脚本，但是不知道是不是程序写的不太完美一次没成功过，看葵牛写了一个py版的，哈哈

0 回复Ta


咸鱼 2017-09-22 09:20:25

我试了一下，7.0.81版本也是可以的

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录