Tomcat7+ 弱口令 && 后台getshell漏洞

环境说明

Tomcat7+权限分为：

- manager（后台管理）
  - manager-gui 拥有html页面权限
  - manager-status 拥有查看status的权限
  - manager-script 拥有text接口的权限，和status权限
  - manager-jmx 拥有jmx权限，和status权限
- host-manager（虚拟主机管理）
  - admin-gui 拥有html页面权限
  - admin-script 拥有text接口权限

这些权限的作用可以查看：http://tomcat.apache.org/tomcat-8.5-doc/manager-howto.html。

在`conf/tomcat-users.xml`文件中配置用户的权限：

```
<?xml version="1.0" encoding="UTF-8"?>
<tomcat-users xmlns="http://tomcat.apache.org/xml"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
              version="1.0">

    <role rolename="manager-gui"/>
    <role rolename="manager-script"/>
    <role rolename="manager-jmx"/>
    <role rolename="manager-status"/>
    <role rolename="admin-gui"/>
    <role rolename="admin-script"/>
    <user username="tomcat" password="tomcat" roles="manager-gui,manager-
script,manager-jmx,manager-status,admin-gui,admin-script" />

</tomcat-users>
```

可见，用户tomcat拥有上述所有权限，密码是`tomcat`。

正常安装的情况下，tomcat8中默认没有任何用户，且manager页面只允许本地IP访问。只有管理员手工修改了这些属性的情况下，才可以进行攻击。

漏洞测试

打开tomcat管理页面`http://your-ip:8080/manager/html`，输入弱密码`tomcat:tomcat`，即可访问后台：

Tomcat Web Application Manager

Message:	OK

Manager

List Applications	HTML Manager Help	Manager Help	Server Status

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	*None specified*	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	*None specified*	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	*None specified*	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	*None specified*	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	*None specified*	Tomcat Manager Application	true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

下面有一个文件上传：

/host-manager	*None specified*	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	*None specified*	Tomcat Manager Application	true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

Context Path (required):
XML Configuration file URL:
WAR or Directory URL:
Deploy

WAR file to deploy

Select WAR file to upload 选择文件 未选择任何文件
Deploy

Diagnostics

Check to see if a web application has caused a memory leak on stop, reload or undeploy

Find leaks This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

SSL connector configuration diagnostics

Connector ciphers List the configured ciphers for each connector

Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/8.0.43	1.7.0_121-b00	Oracle Corporation	Linux	4.19.0-14-amd64	amd64	ba82ec875032	172.19.0.2

上传一个`.war`包即可Getshell。