预警编号：YJ-2017023

恒安嘉新

关于 Apache Tomcat 存在信息泄露与远程代码执行漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 09 月 20 日

1 漏洞描述

2017 年 9 月 20 日，互联网爆出 Apache Tomcat 远程代码执行漏洞（CVE-2017-12615）与信息泄露漏洞（CVE-2017-12616），综合利用漏洞，攻击者可能获取用户服务器上 JSP 文件的源代码，或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。漏洞危害程度为高危(High)。

2 影响范围

根据官方公告情况，两个漏洞影响版本如下：

1) Apache Tomcat 信息泄露漏洞（CVE-2017-12616）影响版本：

Apache Tomcat 7.0.0 - 7.0.80

2) Apache Tomcat 远程代码执行漏洞（CVE-2017-12615）影响版本：

Apache Tomcat 7.0.0 - 7.0.79

3 漏洞原理

Tomcat 是 Apache 软件基金会（Apache Software Foundation）开发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高的场合下被普遍使用，是开发和调试 JSP 程序的首选。

Apache Tomcat 信息泄露漏洞(CVE-2017-12616)产生的原因是 Tomcat 中启用了 VirtualDirContext 所致，攻击者通过发送精心构造的恶意请求，绕过

设置的相关安全限制，或通过获取到由 VirtualDirContext 提供支持资源服务的 JSP 源代码，从而造成代码信息泄露。

Apache Tomcat 远程代码执行漏洞（CVE-2017-12615）产生的原因是 Tomcat 运行在 Windows 操作系统，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）所致，攻击者可通过精心构造的攻击请求数据包向服务器上传包含任意代码的 JSP 文件，JSP 文件中的恶意代码将能被服务器执行。导致服务器上的数据泄露或获取服务器权限。

4 修复建议

建议升级至 Apache Tomcat 7.0.81 版本，官网链接如下：

http://tomcat.apache.org/download-70.cgi#7.0.81