# 0001

漏洞名称：Tomcat代码执行漏洞

漏洞时间：2017-9-20

CVE编号：CVE-2017-12615

影响平台：Windows

影响版本：Apache Tomcat 7.0.0 - 7.0.81

介绍：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。

EXP: CVE-2017-12615-exp

**0002**

漏洞名称：Apache Tomcat上传绕过/远程执行

漏洞时间：2017-10-03

CVE编号：CVE-2017-12617

影响平台：linux windows

影响版本：9.0.1(Beta),8.5.23,8.0.47以及7.0.82之前

介绍：该漏洞会影响启用了HTTP PUT的系统（通过将Default servlet的“read-only”参数初始化为fales）。如果default servlet的read-only参数设置为了false，或者WebDAV servlet 启用了readonly参数，并设置为false。

POC and EXP：CVE-2017-12617（非pocsuit插件）

**0003**

漏洞名称：Windows上的Apache Tomcat远程代码执行

漏洞时间：2019-04-12

CVE-编号：CVE-2019-0232

影响平台：Windows

影响版本：Apache Tomcat 9.0.0.M1至9.0.17，Apache Tomcat 8.5.0至8.5.39，Apache Tomcat 7.0.0至7.0.93

介绍：在启用了enableCmdLineArguments的Windows上运行时，由于JRE将命令行参数传递给Windows的方式存在错误，CGI Servlet容易受到远程代码执行的攻击。

POC or EXP: CVE-2019-0232

**0004**

漏洞名称：Apache Tomcat Ajp协议文件包含漏洞

漏洞时间：2020-02-20

CVE编号：CVE-2020-1938

影响平台：暂无

影响版本：Apache Tomcat<7.0.100、Apache Tomcat <8.5.51、Apache Tomcat<9.0.3

介绍：Apache与Tomcat都是Apache开源组织开发的用于处理HTTP服务的项目，两者都是免费的，都可以做为独立的Web服务器运行。

Apache Tomcat服务器存在文件包含漏洞，攻击者可利用该漏洞读取或包含 Tomcat 上所有 webapp 目录下的任意文件，如：webapp 配置文件或源代码等。

POC or EXP：CNVD-2020-10487-Tomcat-ajp-POC