# 【漏洞复现】Apache Tomcat安全绕过漏洞（CVE-2018-1305）

深信服千里目安全实验室 / 2018-03-02 08:45:39 / 浏览数 16561 安全技术 漏洞分析 顶(2) 踩(0)

---

近日，Apache Tomcat曝出安全绕过漏洞。漏洞的CVE编号为CVE-2018-1305。

Apache Tomcat是由Apache软件基金会下属的Jakarta项目开发的一个Servlet容器，按照Sun Microsystems提供的技术规范，实现了对Servlet和Java Server Page（JSP）的支持，并提供了作为Web服务器的一些特有功能，如Tomcat管理和控制平台、安全域管理和Tomcat阀等。Tomcat很受广大程序员的喜欢，因为它运行时占用的系统资源小，扩展性好，支持负载平衡与邮件服务等开发应用系统常用的功能。

此次Apache Tomcat的安全绕过漏洞出现在Tomcat的部分版本中。Apache Tomcat Servlet注释定义的安全约束，仅在Servlet加载后才应用。由于以这种方式定义的安全约束适用于URL模式及该点下任何URL，因此可能根据Servlet的加载顺序而对某些安全约束不

上面描述的可能过于专业化，准备了一个案例让各位小伙伴们直观的了解一下。

由于触发此漏洞的前提是：

■■■■■■■■■■■Tomcat■■
■■■■■■■■■■■■■■■■■■

据此搭建一套JDK1.8，Apache Tomcat 8.5.24的运行环境。

新建一个Web工程，导入annotations-api.jar（annotations-api.jar是使用注解所需jar包，不导入会报错）等jar包文件。

由于ServletSecurity注释可以直接用来修饰Java Servlet，对Servlet进行类ACL保护，如果在ServletSecurity中添加ServletSecurity注释，在servlet_two中不添加ServletSecurity注释，就可能导致未授权访问，新建servle

通过上面俩文件比较可以清晰地看出，servlet_one前增加了ServletSecurity注释，而servlet_two前没有ServletSecurity注释。
修改web.xml文件如下（在web.xml对servlet给出名称和定制的URL。用servlet元素分配名称，使用servlet-mapping元素将定制的URL与刚分配的名称相关联。）

这里可以明显的看出有两个servlet（servlet_one和servlet_two），servlet_one的访问路径是"/servlet1/"，servlet_two的访问路径是"/servlet1/servlet2"，由于存在漏洞

这个时候直接访问servlet_one的访问路径"/servlet1/"，此时ServletSecurity注解生效，拒绝访问此资源。

在不重启Tomcat的情况下，访问一次servlet_one的访问路径"/servlet1/"后再次访问servlet_two的访问路径"/servlet1/servlet2"时，ServletSecurity注解已经触发，所以无

影响版本

Apache Tomcat 9.0.0.M1-9.0.4，
Apache Tomcat 8.5.0-8.5.27,
Apache Tomcat 8.0.0.RC1 - 8.0.49，
Apache Tomcat 7.0.0 - 7.0.84。

修复建议

由于在不了解对方网站架构的情况下，很容易先触发网站的安全约束，所以此漏洞利用条件困难，不过也建议小伙伴们及时更新到Apache Tomcat 8.5.28，Apache Tomcat 8.0.50，Apache Tomcat 7.0.85版本。

更新链接：

Apache Tomcat 7.0.85:https://tomcat.apache.org/download-70.cgi
Apache Tomcat 8.0.50:https://tomcat.apache.org/download-80.cgi
Apache Tomcat 8.5.28:https://tomcat.apache.org/download-80.cgi
Apache Tomcat 9.0.5:https://tomcat.apache.org/download-90.cgi

参考链接

CVE链接:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1305
Bugtraq链接:https://www.securityfocus.com/bid/103144/discuss


上一篇：某CMS的还是有点意思的无限制注入 下一篇：金融科技SDL安全设计checklist
1. 0 条回复

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

---

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板