Apache Struts 外部实体(XXE)注入漏洞 S2-069（CVE-2025-68493）通告

■ 通告编号	**NS-2026-0001**	■ 发布日期	**2026-01-12**
■ 漏洞危害	**攻击者利用此漏洞，可实现任意文件读取或拒绝服务等。**		
■ **TAG**	Apache Struts、XXE、S2-069、CVE-2025-68493		

一. 漏洞概述

近日，绿盟科技 CERT 监测到 Apache 发布安全公告，修复了 Apache Struts 外部实体(XXE)注入漏洞 S2-069（CVE-2025-68493）；由于 Apache Struts 的 XWork 组件在解析 XML 配置时未进行有效验证，攻击者可通过构造恶意的 XML 数据注入外部实体，从而读取服务器敏感文件、进行服务器端请求伪造或拒绝服务攻击。CVSS 评分 9.8，请相关用户尽快采取措施进行防护。

Apache Struts 是用于创建 Java Web 应用程序的开源框架，旨在为 Java Web 开发提供一个灵活、强大且易于扩展的解决方案，应用非常广泛。

参考链接：

https://cwiki.apache.org/confluence/display/WW/S2-069

二. 影响范围

受影响版本

- 2.0.0 <= Apache Struts <= 2.3.37（EOL）
- 2.5.0 <= Apache Struts <= 2.5.33（EOL）
- 6.0.0 <= Apache Struts <= 6.1.0

不受影响版本

- Apache Struts >= 6.1.1

三. 漏洞检测

3.1 人工检测

使用 maven 打包的项目可通过 pom.xml 查看当前使用的 struts 版本：

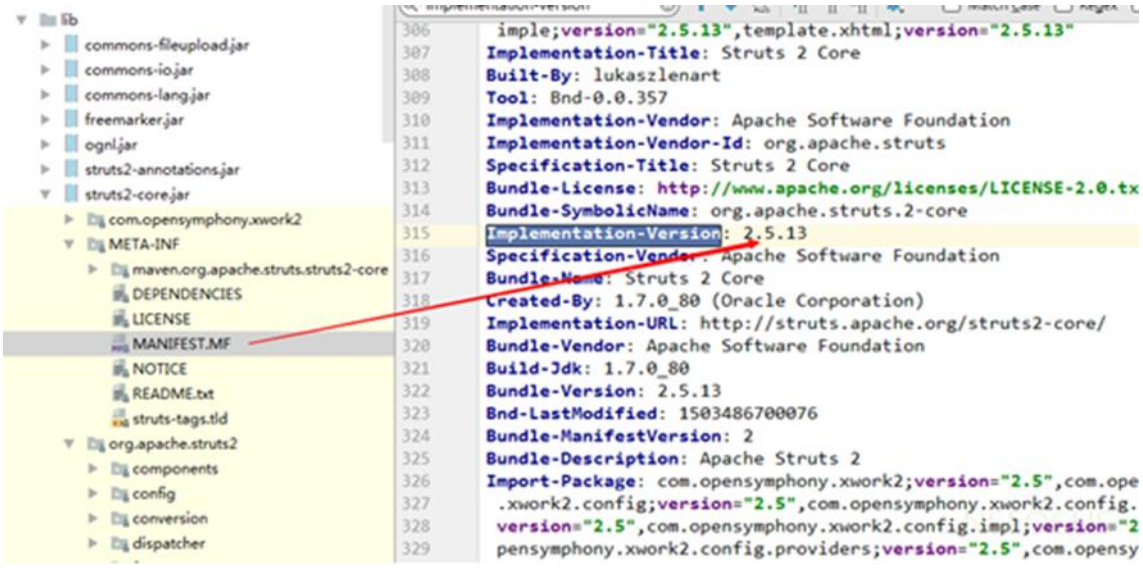
```
<dependency>
    <groupId>javax.servlet</groupId>
    <artifactId>jstl</artifactId>
    <version>1.2</version>
</dependency>

<dependency>
    <groupId>javax.servlet</groupId>
    <artifactId>jsp-api</artifactId>
    <version>2.0</version>
    <scope>provided</scope>
</dependency>

<dependency>
    <groupId>javax.servlet</groupId>
    <artifactId>javax.servlet-api</artifactId>
    <version>3.1.0</version>
    <scope>provided</scope>
</dependency>

<dependency>
    <groupId>org.apache.struts</groupId>
    <artifactId>struts2-core</artifactId>
    <version>2.5.1</version>
</dependency>
```

也可通过查看 lib 中的核心包查看 struts 版本

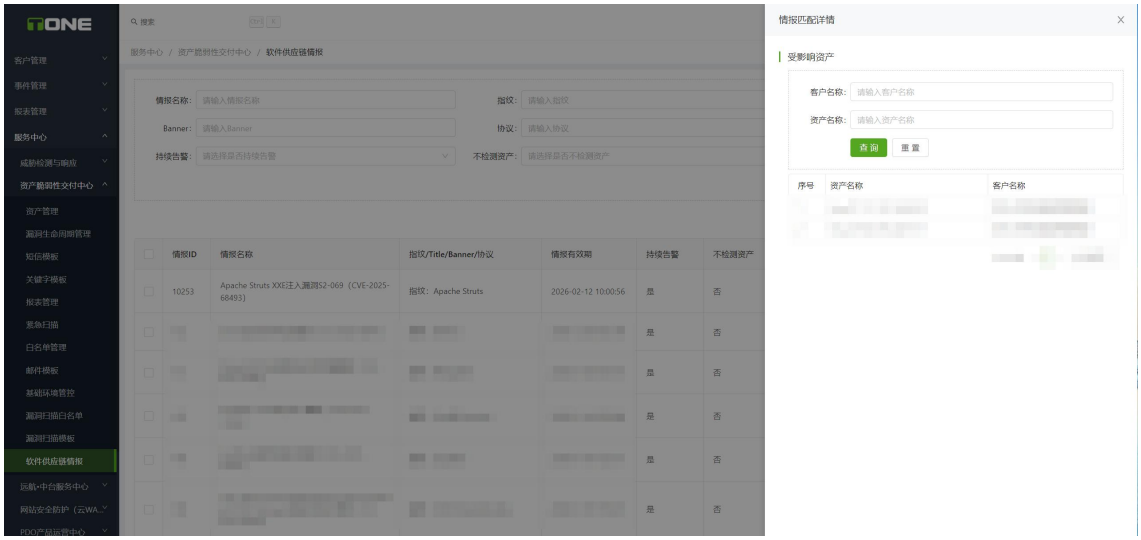


若当前版本在受影响范围内，则可能存在安全风险。

四. 暴露面风险排查

4.1 云端检测

绿盟科技外部攻击面管理服务（EASM）支持 CVE-2025-68493 漏洞风险的互联网资产排查，目前已帮助服务客户群体完成了暴露面排查，在威胁发生前及时进行漏洞预警与闭环处置。



感兴趣的客户可通过联系绿盟当地区域同事或发送邮件至 rs@nsfocus.com 安排详细的咨询交流。

4.2 工具排查

绿盟科技自动化渗透测试工具（EZ）支持 Apache Struts 的服务识别，可直接使用 web 模块进行扫描。（注：企业版请联系绿盟销售人员获取）

```
[*] done_http:7, undo_http:0, undo_port:0, undo_task:0, req:2/34, finger:0, vuln:0
[INF] 2026-01-12 17:33:39 [distribute.go:208] finger: http://[redacted]:18080/struts/
["Apache-Coyote","apache-tomcat"] null
[INF] 2026-01-12 17:33:39 [distribute.go:208] finger: http://[redacted]:18080/ ["apach
e-struts","Apache-Coyote","apache-tomcat"] ["java"]
[*] done_http:7, undo_http:0, undo_port:0, undo_task:0, req:2/37, finger:2, vuln:0
```

工具下载链接：https://github.com/m-sec-org/EZ/releases

新用户请注册 M-SEC 社区（https://msec.nsfocus.com）申请证书进行使用：

五. 漏洞防护

5.1 官方升级

目前官方已发布新版本修复了该漏洞，请受影响的用户尽快升级版本进行防护，下载链接：https://struts.apache.org/download.cgi

5.2 临时防护措施

若相关用户暂时无法进行升级操作，可通过下列措施进行临时缓解：

1、使用自定义 SAXParserFactory 配置，通过设置系统 xwork.saxParserFactory=指向自定义的工厂类，实现默认禁用外部实体；

2、在 JVM 启动参数中配置以下系统属性，可禁用默认 XML 解析器的外部实体访问；

```
-Djavax.xml.accessExternalDTD=""
-Djavax.xml.accessExternalSchema=""
-Djavax.xml.accessExternalStylesheet=""
```

注：设置为空字符串可阻断所有协议。

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。