网络安全预警通报

2026 年第 2 期（总第 60 期）

西安交通大学网络信息中心 2026 年 01 月 28 日

【预警类型】高危预警

【预警内容】

Apache Struts XWork 组件 XML 外部实体注入漏洞（CVE-2025-68493）高危利用风险通报

一、漏洞概述

近日，安全研究人员披露 Apache Struts 框架中 XWork 组件存在一处 XML 外部实体注入(XXE)漏洞,漏洞编号为 CVE-2025-68493。该漏洞源于 XWork 在解析 XML 配置文件和请求相关 XML 数据时，未对外部实体（External Entity）进行有效限制和安全校验，导致解析过程中可被注入恶意外部实体引用。

在漏洞被成功利用的情况下，攻击者可通过构造特定的恶意 XML 数据，触发服务器解析外部实体，从而读取服务器本地敏感文件、探测内网资源，甚至发起服务器端请求伪造（SSRF）攻击。同时，

恶意构造的 XML 还可能导致 XML 解析过程资源耗尽，引发拒绝服务（DoS）风险。

Apache Struts 作为企业级 Web 应用中广泛使用的框架，一旦存在可被远程触发的 XXE 漏洞，极易被攻击者利用进行自动化扫描和批量攻击，安全风险较高，建议相关单位尽快开展排查和加固工作。

二、漏洞详情

1.技术原理

漏洞类型：XML 外部实体注入（XXE）

漏洞等级：高危

产生原因：

Apache Struts 的 XWork 组件在处理 XML 配置文件及部分 XML 请求数据时，使用了不安全的 XML 解析方式，未显式禁用外部实体和 DTD 声明。攻击者可在 XML 内容中定义外部实体，并在解析阶段被服务器自动解析和访问。

当解析器在服务器高权限环境下运行时，外部实体可指向本地文件或内部网络地址，从而造成敏感信息泄露、内网探测或间接攻击第三方系统。

2.利用条件

- 目标系统使用 Apache Struts 框架
- XWork 组件处于受影响版本范围内
- 存在可控的 XML 解析入口（如配置加载、接口请求等）
- 攻击者可通过网络访问相关 Web 服务

关联风险：

- 服务器敏感文件（如配置文件、密钥信息）泄露
- 利用 SSRF 访问内网服务或云平台元数据接口
- 触发拒绝服务，影响业务系统稳定性

三、漏洞影响范围

1. 受影响版本

Apache Struts 2.0.0≤版本≤2.3.37（2.3.x 分支已停止维护）

Apache Struts 2.5.0≤版本≤2.5.33（2.5.x 分支已停止维护）

Apache Struts 6.0.0≤版本≤6.1.0

2. 受影响系统

1）基于 Apache Struts 构建的 Web 应用系统

2）高校、政企单位内部管理系统

3）对外提供服务的业务平台及门户网站

3.威胁严重性

该漏洞可被远程触发，利用成功后可造成信息泄露、SSRF 及拒绝服务等多种安全影响。综合漏洞影响范围和利用价值，安全风险评估为高危，建议按较高等级进行应急处置。

四、处置建议

1.立即将 Apache Struts 升级至官方已修复版本，建议升级至 Apache Struts 6.1.1 及以上版本。

2.开展全面资产排查，确认是否存在使用 Apache Struts 的存量系统，并重点关注对外暴露的业务应用。