

云平台信息安全通告 2020(第 012 号)

关于 Apache Struts 2 远程代码执行漏洞 S2-059 (CVE-2019-0230) 的安全通告

Apache Struts 是美国 Apache 软件基金会负责维护的一个开源项目，是一套用于创建企业级 Java Web 应用的开源 MVC 框架，主要提供两个版本框架产品，Struts 1 和 Struts 2。Apache Struts 2 是 Apache Struts 的下一代产品，是在 Struts 1 和 WebWork 的技术基础上进行合并的全新 Struts 2 框架。

Apache Struts 于 2020 年 8 月 13 日披露了 Struts 2 远程代码执行漏洞 (S2-059/CVE-2019-0230)，Struts 2 会对某些标签的属性值进行二次表达式解析，当使用%{...}或\${...}语法对标签属性进行强制解析的情况下，攻击者通过精心构造的请求，可能造成远程代码执行。

一、影响范围

- Struts 2.0.0 - Struts 2.5.20

二、漏洞检测

用户可通过版本检测的方式判断当前应用是否存在风险。

三、修复建议

1. 升级到 Apache Struts 2.5.22 或更高版本。

参考链接：

<https://cwiki.apache.org/confluence/display/WW/S2-059>

<https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.22>

请各业务单位重点关注，及时排查，防止发生安全事件！如有疑问，请联系星云大数据政务数据支撑部（福建省电子政务云平台安全中心），联系电话：18065137002，18695617964。