网络安全风险预警通报

2020 年第 3 期 （总第 12 期）

广西大学网络信息中心 2020 年 12 月 30 日

【预警类型】 高危预警

【预警内容】

Apache Struts2 存在远程代码执行漏洞（S2-061）的安全公告

安全公告编号 CNTA-2020-0026

一、漏洞概述

Struts2 是第二代基于 Model-View-Controller（MVC）模型的 java 企业级 web 应用框架，成为国内外较为流行的容器软件中间件。Apache Struts2 远程代码执行漏洞(CNVD-2020-69833，对应 CVE-2020-17530)。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞细节已公开，厂商已发布升级版本修复此漏洞。。

二、漏洞详情

2020 年 12 月 8 日，Apache Strust2 发布最新安全公告，

Apache Struts2 存在远程代码执行的高危漏洞（CVE-2020-17530）。由于 Struts2 会对一些标签属性的属性值进行二次解析，当这些标签属性使用了 `%{x}` 且 `x` 的值用户可控时，攻击者利用该漏洞，可通过构造特定参数，获得目标服务器的权限，实现远程代码执行攻击。

三、漏洞影响范围

漏洞影响的产品版本包括：

Struts 2.0.0-2.5.25

四、漏洞处置建议

经综合技术研判，该漏洞的利用条件较高，难以进行大规模利用。Apache 公司已发布了新版本（2.5.26）修复了该漏洞，CNVD 建议用户及时升级至最新版本：

https://cwiki.apache.org/confluence/display/WW/S2-061

附：参考链接：

https://cwiki.apache.org/confluence/display/WW/S2-061