预警编号：YJ-2017032

恒安嘉新

关于 Apache Struts2 存在 S2-054 拒绝服务漏洞与 S2-055 反序列化漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 12 月 04 日

1 漏洞描述

2017年12月1日，Apache Strusts 官方发布了Struts2的两个中危漏洞，分别是：S2-054 拒绝服务漏洞（CVE-2017-15707），S2-055 反序列化漏洞（CVE-2017-7525），攻击者可利用上述漏洞对目标系统进行 Dos 攻击或反序列化代码执行攻击。该框架在国内使用非常广泛。漏洞危害程度为中危。

2 影响范围

Struts 2.5 – Struts 2.5.14

3 漏洞原理

Struts2 是 Apache 软件基金会负责维护的一个基于 MVC 设计模式的 Web 应用框架开源项目。2017 年 12 月 1 日爆出的两起漏洞细节如下：

S2-054 拒绝服务漏洞：Apache Struts REST 插件使用了过时的 JSON-lib 库，攻击者可以通过构造特制的 JSON 恶意请求造成 DOS 攻击。

S2-055 反序列化漏洞：由于 Apache Struts 调用了存在反序列化漏洞的 Jackson JSON 库，导致反序列化漏洞的产生。

4 修复建议

S2-054 修复建议：

方法一：升级到 Apache Struts 版本 2.5.14.1。

方法二 :使用 Jackson 处理程序替换默认的 JSON-lib 处理程序 ,替换方法：

http://struts.apache.org/plugins/rest/#use-jackson-framework-as-json-contenttypehandler

S2-055 修复建议：

方法一：升级到 Apache Struts 版本 2.5.14.1。

方法二：手动将项目中的 com.fasterxml.jackson 升级到版本 2.9.2，详情参考：https://github.com/FasterXML/jackson-databind/issues/1599#issuecomment-342983770