预警编号：YJ-2018015

恒安嘉新

关于 Apache Struts2 S2-057

存在远程代码执行漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2018 年 8 月 23 日

1 漏洞描述

2018 年 8 月 22 日，Apache Software Foundation 官网爆出 Apache Struts2 S2-057 远程代码执行漏洞。攻击者利用该漏洞远程执行代码。该漏洞危害程度为高危(High)。目前，漏洞利用细节暂未公开，厂商已发布了漏洞修复补丁。

2 影响范围

目前，官方披露的受影响版本如下（包括但不限于）：

Struts 2.3-2.3.34

Struts 2.5-2.5.16

3 漏洞原理

Struts2 是第二代基于 Model-View-Controller(MVC)模型的 java 企业级 web 应用框架，并成为国内外较为流行的容器软件中间件。

漏洞触发条件如下：

1、定义 XML 配置时 namespace 值未设置且上层动作配置（Action Configuration）中未设置或用通配符 namespace。

2、url 标签未设置 value 和 action 值且上层动作未设置或用通配符 namespace。

4 修复建议

目前，厂商已发布了最新版本修复了漏洞，具体修复建议如下：

1.建议升级到 Struts 2.3.35 或 Struts 2.5.17。

2.如无法及时升级，还可采用如下临时解决方案:

当上层动作配置中未设置或使用通配符 namespace 时，验证所有 XML 配置中的 namespace，同时在 JSP 中验证所有 url 标签的 value 和 action。

附：参考链接：

https://cwiki.apache.org/confluence/display/WW/S2-057