预警编号：YJ-2017017

恒安嘉新

关于 Struts(S2-048)远程命令执行漏洞

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 07 月 07 日

1 漏洞描述

2017 年 7 月 7 日，Apache Struts 发布最新的安全公告，漏洞编号为 S2-048，CVE 编号：CVE-2017-9791。该漏洞存在 Struts2 和 Struts1 一个 Showcase 插件 Action Message 类中，通过构建不可信的输入实现远程命令攻击，存在安全风险，漏洞危害程度为高危(High)。

2 影响范围

Struts 2.3.x

3 漏洞检测

自查 Struts 框架版本查看 struts.jar/META-INF/MANIFEST.MF 再查看 Implementation-Version 看后面的数字。

4 修复建议

- 关闭 Showcase 插件
- 建议升级到最新版本 2.5.10.1
- 开发者通过使用 resource keys 替代将原始消息直接传递给 ActionMessage 的方式。 如下所示：

  messages.add("msg", new ActionMessage("struts1.gangsterAdded", gform.getName()));

不要使用如下的方式：

```
messages.add("msg", new ActionMessage("Gangster " + gform.getName()
+ " was added"));
```