预警编号：YJ-2017021

恒安嘉新

关于 Apache Struts2 REST 插件存在 S2-052 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 09 月 06 日

1 漏洞描述

2017 年 9 月 5 日 ,互联网爆出 Apache struts2 S2-052 远程代码执行漏洞（CVE-2017-9805）。攻击者可以通过构造恶意 XML 请求在目标服务器上远程执行任意代码，获得服务器权限。目前相关利用代码已在互联网公开并传播，有可能导致互联网上大规模的攻击尝试。该漏洞危害程度为高危(High)。

2 影响范围

Struts 2.5 – Struts 2.5.12 版本

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。Xstream 是一种 OXMapping 技术，是用来处理 XML 文件序列化的框架,在将 JavaBean 序列化或将 XML 文件反序列化的时候，不需要其它辅助类和映射文件。Xstream 也可以将 JavaBean 序列化成 JSON 或反序列化，使用非常方便。

Struts2 的 REST 插件使用带有 XStream 例程的 XStreamHandler 执行反序列化操作，但在反序列化过程中未做任何类型过滤，导致攻击者可能在反序列化 XML 负载时构造恶意的 XML 内容执行任意代码。

4 修复建议

- 建议尽快升级到 2.5.13 版本。
- 如果非网站功能需要，建议删除 Struts REST 插件，或仅限于服务器普通页面和 JSONs <constantname="struts.action.extension" value="xhtml,,json" />
- 限制服务端扩展类型，删除 XML 支持。

关于兼容：

由于可用类的默认限制，某些 REST 操作可能会影响到正常的网站功能。在这种情况下，请调查介绍的新接口以允许每个操作定义类限制，这些接口是：

org.apache.struts2.rest.handler.AllowedClasses

org.apache.struts2.rest.handler.AllowedClassNames

org.apache.struts2.rest.handler.XStreamPermissionProvider