Struts2 方法调用远程代码执行漏洞(S2-032)

2016 年 4 月 21 日 Struts2 官方发布两个 CVE，其中 CVE-2016-3081 官方评级为高。主要原因为在用户开启动态方法调用的情况下，会被攻击者实现远程代码执行攻击。

该漏洞从 4 月 25 日开始，在国内引起了广泛的关注，各大安全厂商陆续发布了相关的安全公告。中国网安·安全云中心已经对我们服务客户的网站（8000 多个）进行该漏洞的安全检测，本次检测结果如下：

1. 我们服务客户主要集中在政府、教育、国有企事业单位三大行业，其中 90%以上的网站是用 Windows 操作系统、87%的网站开发语言为 Asp.NET；
2. 本次检测中仅有 1%的网站使用了 StructⅡ架构，在发现该架构的网站中，教育行业网站占比 48%、政府行业网站占比 42%、企事业单位网站占比 10%；
3. 在所有检测结果中，仅有 1 个上海区域的网站存在此类漏洞风险，中国网安·安全云中心已经通知该客户。

中国网安·安全云中心
2016 年 5 月 2 日

漏洞介绍

1. 基本情况

SSV ID:	SSV-91389	CVE-ID:	CVE-2016-3081
提交时间:	2016-04-21	威胁等级:	高
漏洞类别:	代码执行		

2. 漏洞描述

2016 年 4 月 21 日 Struts2 官方发布了 Apache Struts 2 任意代码执行漏洞（CVE-2016-3081, S02-32），该漏洞主要原因为在开启动态方法调用(DMI)的情况下，黑客可以利用漏洞直接执行任意代码，该漏洞影响的 struts 版本包括 Struts 2.0.0 - Struts2.5.BETA3 (不包括已修复版本：2.3.20.2、2.3.24.2、2.3.28.1)。

3. 漏洞危害

Apache Struts 2 任意代码执行漏洞（CVE-2016-3081, S02-32）属于高危险漏洞，据乌云平台漏洞报告，目前漏洞利用代码已经被强化，可直接通过浏览器的提交对服务器进行任意操作并获取敏感内容。Struts 漏洞影响巨大，受影响站点以电商、银行、门户、政府居多，而且一些自动化、傻瓜化的利用工具开始出现，填入地址可直接执行服务器命令，读取数据甚至直接关机等操作。

4. 漏洞影响范围

Struts 2.0.0 - Struts2.5.BETA3

(不包括已修复版本：2.3.20.2、2.3.24.2、2.3.28.1)

5. 漏洞修复方法

a) 关闭动态方法调用

- 开放商确认关闭该功能是否对应用系统业务有影响，若影响正常业务运行，则采用第二种修复方法。
- 修改 Struts2 的配置文件 struts.xml，该文件默认目录为 src/struts.xml，将“struts.enable.DynamicMethodInvocation” 设置为 false，如：<constant name="struts.enable.DynamicMethodInvocation" value="false" />;

b) 升级 Struts 版本

将 Struts 版本至 Struts 2.3.20.2, Struts 2.3.24.2 或者 Struts 2.3.28.1 以上版本，参考链接：https://struts.apache.org/download.cgi#struts23281

备注：升级包可以自行从互联下载，亦可致电上海三零卫士，我们的技术人员会提供给您。

6. 修复注意事项

为了降低修复所造成的风险，建议采取以下措施：

a) 漏洞升级包必须来自官方发布。

b) 选择非工作时间实施修复工作。

c) 实施前，将应用系统、重要数据库进行全备份工作。

d) 实施前，建议搭建测试环境，在测试环境成功实施后，再正式开始实施。

e) 实施过程中，需要应用系统开发商提供相关人员进行后台支持，一旦出现异常，配合进行回退工作。

f) 修复完成后，对应用系统各项功能进行测试，并在后期持续进行观察。