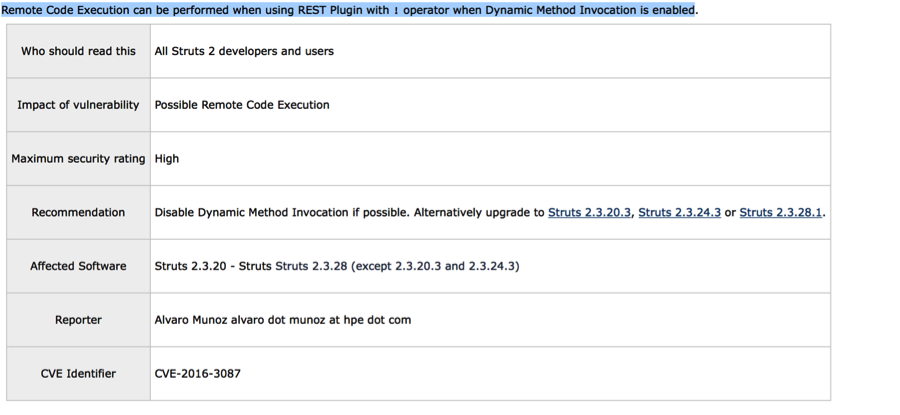
Struts2 S2-033漏洞分析

1.介绍

Struts 2是Struts的下一代产品，是在 struts 1和WebWork的技术基础上进行了合并的全新的Struts 2框架。其全新的Struts 2的体系结构与Struts 1的体系结构差别巨大。Struts 2以WebWork为核心，采用拦截器的机制来处理用户的请求，这样的设计也使得业务逻辑控制器能够与 ServletAPI完全脱离开，所以Struts 2可以理解为WebWork的更新产品。虽然从Struts 1到Struts 2有着太大的变化，但是相对于WebWork，Struts 2的变化很小。

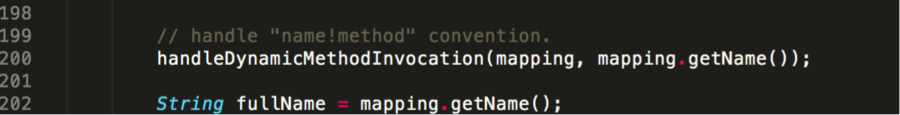
2. 关于S2-033分析

就是当启用动态方法调用之后，使用了rest插件就可能执行ognl表达式导致任意代码执行。

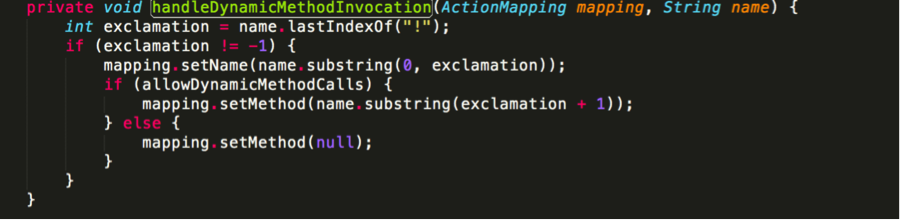
[](http://seclab.dbappsecurity.com.cn/wp-content/uploads/2016/06/1.png)

Rest插件使用了之后，ActionMapping是通过org.apache.struts2.rest. RestActionMapper.java的public ActionMapping getMapping(HttpServletRequest request,ConfigurationManager configManager)的方法获取的。

其中会通过handleDynamicMethodInvocation方法设置ActionMapping的method属性。

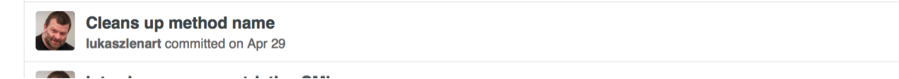
[](http://seclab.dbappsecurity.com.cn/wp-content/uploads/2016/06/2.png)

获取uri中!后面的内容作为ActionMapping的method属性。但是这个method属性未做任何处理。导致了后面的代码执行。

[](http://seclab.dbappsecurity.com.cn/wp-content/uploads/2016/06/3.png)

后面的执行流程跟之前分析的S2-032漏洞执行流程一致(<http://seclab.dbappsecurity.com.cn/?p=924>).都是将ActionMapping的属性设置到ActionProxy中，然后从ActionProxy中获取method属性带入到ognl表达式中执行。从而导致任意代码执行。

分析github上的修复的版本Struts 2.3.20.3, Struts 2.3.24.3 or Struts 2.3.28.1，发现跟之前版本没有多大改动，然后查看Struts2 2.5版本的提交纪录，发现一条更新纪录。

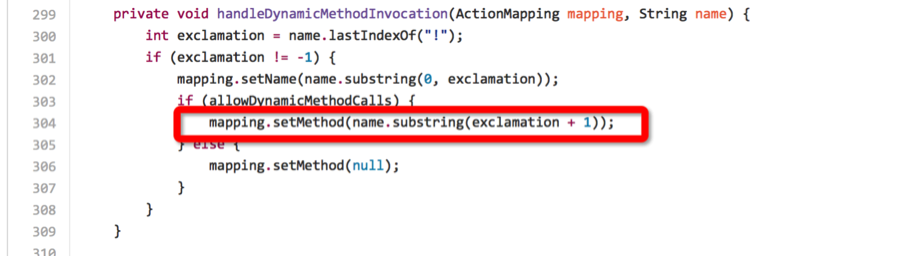
[](http://seclab.dbappsecurity.com.cn/wp-content/uploads/2016/06/4.png)

[](http://seclab.dbappsecurity.com.cn/wp-content/uploads/2016/06/5.png)

过滤了struts2-rest插件中RestActionMapper.java的handleDynamicMethodInvocation中的actionMethod属性

但是分析到安全公告中的修复版本根本对这个漏洞未做任何修补。

如下图:

[](http://seclab.dbappsecurity.com.cn/wp-content/uploads/2016/06/6.png)

官方安全公告中的最新版修复是无效的。

修复方案：关闭动态方法调用

在struts.xml中的<constant name=”struts.enable.DynamicMethodInvocation” value=”true” />改为<constant name=”struts.enable.DynamicMethodInvocation” value=”false” />如果不存在上面的属性 则不用修改，或者升级到Struts2 2.5