远程代码执行漏洞的探讨

2016-05-27 京东安全应急响应中心

安全小课堂第十二期

远程代码执行是我的一把备用钥匙，你的一不留神我就能轻易出入你们家，运气好赶上框架级应用那备用钥匙就不是一把了，甚至提权伪装成宿主去操控一切。

远程代码执行漏洞因其简单粗暴的特点，流行于各大黑客圈。本期，咱们邀请到了360安全专家genxor和唯品会安全专家张剑，来和大家聊一聊远程代码执行漏洞。☺

1

豌豆妹

能说说远程代码执行漏洞的原理么？

小新 

由于开发人员编写源码，没有针对代码中可执行的特殊函数入口做过滤，导致客户端可以提交恶意构造语句提交，并交由服务器端执行。命令注入攻击中WEB服务器没有过滤类似system(),eval()，exec()等函数是该漏洞攻击成功的最主要原因。

豌豆妹

那现状呢？

小丸子

因其简单粗暴的特点，流行于各大黑客圈。现在最主要的，也是目前案例最多的，可能是struts2的利用了。再就是去年的java反序列。反序列化这个东西， 其实是一门老手艺了，很久以前php就流行过相关利用，具体可以参看super hei、fly。比如php里面unserialize函数的利用。系统层面早期的栈溢出，MS03-026、MS04-011、MS05-039、MS06-040、MS08-067。

葫芦娃

远程代码执行出现的范围较广，一般的应用程序，如浏览器，adobe flash player，还有操作系统都会有相关的漏洞导致远程代码执行。近年来远程代码执行方面的漏洞，出镜最多的可能就属struts2了，这个框架在国内应用于各大门户网站。现在android也出现了很多远程代码执行的漏洞。像堆溢出，栈溢出，整型溢出，类型混淆，use after free，访问越界，格式化字符串等都会导致远程代码执行。

2

豌豆妹

那远程代码执行漏洞出现的形式有哪些呢？

哆啦A梦

web层面先说java。比如利用表达式注入、调用反射类、xslt注入、服务端模板注入、操控容器的classLoader等。php层面的话，比如利用一些危险函数比如system、shell_exec、passthru等。

小新

还有一种形式，就是shellshock那种漏洞，bash的命令执行，实际上是加载不安全的环境变量导致，bash的代码底层在解析环境变量的时候出现问题，导致可以注入任意代码，这个漏洞有点儿类似于php里面的create_function命令执行漏洞，根源都是由于底层函数对用户传入的变量没有严格过滤，导致命令注入。

3

豌豆妹

大家都知道远程代码执行漏洞都是简单粗暴，能详细给说说危害到底有多大么？

小丸子

命令执行，对于攻击者来说是打开缺口的绝好方法，可长驱直入控制内网，甚至脱裤。

葫芦娃

危害概述就是攻击者可以通过远程调用的方式来让被攻击计算机设备执行恶意程序，从而控制远程计算机；从危害范围来讲，远程代码执行漏洞的影响范围很广，例如去年关于安卓libStagefright的一系列漏洞号称影响95%安卓手机的安全，攻击者只需给受影响系统发送条彩信就可以控制手机。

4

豌豆妹

那如何预防远程代码执行漏洞的侵入呢？能说说防御措施么。

小新 

开发程序时，要假定所有输入都是可疑的，尝试对所有输入提交可能执行命令的构造语句进行严格的检查或者控制外部输入，系统命令执行函数的参数不允许外部传递。

哆啦A梦 

简单来说，卡住入口点很关键。对输入的数据不仅要验证数据的类型，还要验证其格式、长度、范围和内容。

小丸子 

我举个比较详细的例子。拿struts2来举例。在执行ognl之前设置黑名单，在struts-default.xml配置struts.excludedClasses限制一些类。也就是说，卡住ognl的入口，设置黑名单，过滤其执行命令的通道。除了安全编码，在安全应急时，要抓住漏洞特征，快速定位有漏洞的程序和系统；在补丁程序未开发完时，抓住攻击代码特征，对远程输入数据进行分析，验证；及时更新程序，打补丁；其他的方法就是常规的waf之类了。

5

豌豆妹

能给大家分享下遇到过的比较典型的案例么？

哆啦A梦

我就以我的理解总结下wooyun上的三星默认输入法远程代码执行。

豌豆妹

愿闻其详。□

哆啦A梦

攻击前提是攻击者能够劫持流量：首先，该输入法在更新语言包时，对下载的文件校验不严格，没有签名，中间人可以同时篡改下载文件和对应的hash值绕过校验；然后，语言压缩包中的文件是由 system user写入的，有很高的权限，可以写入很多位置；再者，odex文件完整性校验机制有问题，只是校验odex文件的crc32和modify time；由以上第二点，包含在语言zip包中的恶意odex文件就可以覆盖/data/dalvik-cache/目录下的odex；由第三点，保证恶意odex的crc32和modify time和源odex文件一致，绕过odex文件校验，以system user权限执行恶意的odex。

豌豆妹

hhha~感谢360安全专家genxor和唯品会安全专家张剑，与我们分享宝贵经验，撒花~~□咱们下期再见！

安全小课堂往期回顾：

1、论安全响应中心的初衷；
2、安全应急响应中心之威胁情报探索；
3、论安全漏洞响应机制扩展；
4、企业级未授权访问漏洞防御实践；
5、浅谈企业SQL注入漏洞的危害与防御；
6、信息泄露之配置不当；
7、XSS之攻击与防御；
8、电商和O2O行业诈骗那些事儿（上）；
9、电商和O2O行业诈骗那些事儿（下）；
10、CSRF的攻击与防御；
11、账户体系安全管理探讨。

jsrc_team

京东安全应急响应中心

动动手指，关注下呗~□