Java反序列化漏洞

2015 年11月6日,FoxGlove Security安全团队的@breenmachine 发布的一篇博客[3]中介绍了如何利用Java反序列化漏洞,来攻击最新版的WebLogic、WebSphere、JBoss、Jenkins、 OpenNMS这些大名鼎鼎的Java应用,实现远程代码执行。

然 而事实上,博客作者并不是漏洞发现者。博客中提到,早在2015年的1月28号,Gabriel Lawrence (@gebl)和Chris Frohoff (@frohoff)在AppSecCali上给出了一个报告[5],报告中介绍了Java反序列化漏洞可以利用Apache Commons Collections这个常用的Java库来实现任意代码执行,当时并没有引起太大的关注,但是在博主看来,这是2015年最被低估的漏洞。

确 实,Apache Commons Collections这样的基础库非常多的Java应用都在用,一旦编程人员误用了反序列化这一机制,使得用户输入可以直接被反序列化,就能导致任意代 码执行,这是一个极其严重的问题,博客中提到的WebLogic等存在此问题的应用可能只是冰山一角。

虽 然从@gebl和@frohoff的报告到现在已经过去了将近一年,但是@breenmachine的博客中提到的厂商也依然没有修复,而且国内的技术人 员对这个问题的关注依然较少。为了帮助大家更好的理解它,尽快避免和修复这些问题,本文对此做了一个深入的漏洞原理和利用分析,最后对上面提到的这些受影 响的应用,在全球范围内做一个大概的统计。

<https://github.com/foxglovesec/JavaUnserializeExploits>

https://github.com/frohoff/ysoserial