Java攻击隐患难除安全不容忽视 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/245/2021_2022_Java_E6_94_BB_E5_87_BB_c104_245770.htm 最值的重视的问题是关于Java与外部的接口的。年初的时候人们发现QuickTime的Java接口存在一系列高调的安全漏洞。在最近几个月中， Java Web Start（帮助客户机端应用程序开发的一个新技术）技术也被发现了一连串的弱点。关于这些案件的新闻都是关于漏洞的而没有提及开发。 早在2004年，Sun公司在各种浏览器和操作系统中运行Java程序的一个插件被发现存在一个安全漏洞。这个安全漏洞能够让病毒通过 Windows和Linux电脑进行传播。安全信息提供商Secunia公司在安全公告中把这个安全漏洞列为“ 高危 ”等级。这个Java插件能够让小型网络程序在用户计算机上安全的运行。但是，这个安全漏洞允许恶意网站绕过安全措施通过受害者的浏览器在用户计算机上运行恶意程序。由于这一过程无需用户干预，因此这是“ 严重 ”等级的安全漏洞。而且，这个安全漏洞可以被用来攻击Windows和Linux等各种操作系统，因此就更加严重。 一些纯粹基于Java的开发，生产出在non-VM软件中易于被攻击的同一类型的软件业务。考虑近期Java的图像解析代码的弱点，我们发现来自文件的解析数据似乎是一个在所有平台永不休止的安全问题源头。但很多这类问题，因为存在于不太知名的应用程序，所以即使它们被正确发现并被供应商所确定也仍然在很大程度上未被公众所了解。 Java是一个互联网技术中的一个相关的标准部分，恶意程序作者似乎逐渐开始关注它。我曾见过其他的关于恶意Java代码的公开报告，比如一份来

自ISC的报告。这可能是因为将Java作为开发平台的工作刚刚起步。Java的堆管理使之能够被用来开发喷涂堆代码。如果这些都可以在很大程度上被可靠的操作，即使只工作充足时间的50%Java也是游走在麻烦的边缘。我也不清楚重写Java的堆管理来解决问题是否会造成实际的Java代码兼容性问题。 针对处理Java安全问题的建议是令人不安的老生常谈：及时升级Java，使用IDS /IPS（入侵检测系统/入侵防御系统）和保持签名的最新性，不要浏览不安全的网站等，这些和针对非Java产品的建议没有什么区别。但是难道不应该有所区别吗？