开启Windows的DEP和ASLR安全功能很重要 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E5_BC_80_E5_90_AFWind_c100_644843.htm 问：最近读到Secunia安全公司的一则调查报告，报告显示许多应用程序在较新版的windows中没有使用核心的安全功能：地址空间布局随机化（ASLR）和数据执行保护技术（DEP）。您对这种现象有何见解？如何确保我们的内部程序开发者了解这些功能的使用？ 答：在我回答你的问题之前，我想先解释一下什么是地址空间布局随机化（ASLR)和数据执行保护（DEP）。ASLR的作用是，将系统代码的入口数据点分散在内存中，这样入口数据点的位置就处于不可预测的位置。这种情况下，恶意代码访问系统时就难以定位系统功能的位置。例如，今天启动电脑时，wsock32.dll在物理内存的位置是0x73200000，明天这个位置就可能是0x779b0000。DEP是一系列的软件安全检查，利用Windows中的异常处理机制和执行数据页中的代码两项技术来阻止恶意代码。 然而，这些安全特征只有在开发者将它们与应用程序结合的情况下才能发挥作用。Secunia的报告显示，许多软件应用程序并不支持这些安全功能，开发者也不能很好的使用这些安全功能。报告报出时，Java、Apple QuickTime、Foxit Reader、Google Picasa、OpenOffice.org 、RealPlayer和VLC media player都没能与DEP或ASLR整合。由此看来，许多恶意的黑客攻击应用程序而不是Windows系统本身是有深层原因的。Windows系统充分利用了DEP和ASLR的安全功能。令人欣慰的是，该报告公布后，有些供应商在最近的补丁里增添了对这些安全选项的支持，有的也正在致

力于改进这一情况。 在我看来，许多组织没有采用Windows DEP或ASLR安全功能是基于对时间和财力的考虑。但是，让企业开发者学习如何将这些安全控制和内部的应用程序相结合是一个好的建议。企业中的开发者如果使用微软的Visual Studio，那么要执行这两项安全功能就很容易了，执行的过程也会被很好地记录。许多在线的资源介绍了将安全功能与应用程序整合的方法。Visual C Team Blog涉及到如何设置连接器选择/DYNAMICBASE和/NXCOMPAT：/DYNAMICBASE用来修改执行程序的数据头，来显示该程序在操作系统加载时是否需要随意的重定基底。ASLR和/NXCOMPAT用来指定那些与DEP兼容的可执行程序。用户可以在Visual Studio里清晰地对这两项选择进行设置；默认的设置是“ 开启 ”。 Windows Vista SP1、Windows XP SP3和Windows Server 2008加入了一个新的API，即Set Process DEP Policy，它允许开发者在运行时间设置DEP而不是使用连接器选项。微软的Michael Howard在他的博客中更加详细的解释道，MSDN Library有一些关于编程注意事项和应用程序兼容性的问题，并且在使用这些安全控制时你也要考虑这些问题。 ASLR和DEP是两项企业应当与自身的应用程序相结合的安全功能。为此，微软提供了大量的关于如何整合的信息，即使这些信息对开发者而言较新颖，可是难度并不大。另外，应用程序会因为与安全特征的结合而变得更加安全。 百考试题温馨提示：本内容来源于网络，仅代表作者个人观点，与本站立场无关，仅供您学习交流使用。其中可能有部分文章经过多次转载而造成文章内容缺失、错误或文章作者不详等问题，请您谅解。如有侵犯您的权利，请联系我们，本站会立即予以处理。 相关推

荐： #0000ff>Windows8可能会是云端运行的操作系统？ #0000ff>Windows7自带功能完成磁盘数据加密 #0000ff>解决Windows7游戏花屏问题 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com