困扰Windows17年的安全缺点揭秘Microsoft认证考试 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_9B_B0_E6_89_B0Wind_c100_644395.htm 微软在 2009年6月22 确认了一个从 17 年前 Windows 操作系统以来直到目前都还存在的一个安全性弱点，他能让不受信任或无权限的用户轻易的进入系统核心(system kernel)并取得该系统最大权限，目前尚无任何补丁(Patch)可以修正这个问题，但还是有方法可以强化你系统的安全性。 这个弱点是利用一个在 Windows 中称为 Virtual DOS Machine (VDM) 的功能，这功能是为了向前兼容 16-bit 应用程序的执行而设计的，这个功能在所有 32-bit 版的 Windows 都有支持 (64-bit 操作系统无此问题)，由于此功能从 1993 年开始就有了，所以从 Windows NT 3.1, XP, 2000, Server 2003, Vista, Server 2008, 甚至是 Windows 7 都一样有这个弱点，黑客只要能利用 VDM 功能写一点点程序就可以轻松入侵你的计算机，且 PoC 的原代码也已经放出来了。 要解决这个问题也很容易，只要关闭 MSDOS 与 WOWEXEC 子系统即可有效避免弱点被有心人士利用，现在还有人在用 16-bit 应用程序的人应该不多了吧？但也许有些老公司还在用祖母级的 ERP 或进销存程序也不一定。 解决此问题最简单的方式就是通过 Active Directory (AD) 设定组策略，限制网域内所有计算机执行 16-bit 应用程序。 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