Windows17年的老漏洞(VDM0day)须警惕计算机等级考试
PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/645/2021_2022_Windows17_E5_c98_645208.htm 这个 漏洞发生于内核处理VDM(Virtual DOS Maching)的过程中，VDM是微软为了兼容老式的16位MS-DOS程序而存在于Windows中的一个子系统。受这个漏洞影响的版本包括 - Windows 2000 - Windows XP - Windows Server 2003 - Windows Vista - Windows Server 2008 - Windows 7 从网上正在扩散的攻击代 码可以知道，黑客可以利用该漏洞成功完成提权。这个漏洞的利用前提 是，必须首先有本地登录的权限。当一般用户已经成功在本地登录后，若接收运行远程黑客的攻击程序，也会造成严重后果。 当然，如果黑客用传统的 挂马来传播的话，是不会得逞的。对于金山网盾的用户来说，想 用这招控制用户的电脑，还得靠捆绑或欺骗。但话说回来了，如果可以欺骗网民运行攻击者的程序，又何必利用这个漏洞呢，这样做就有画蛇添足的嫌疑了。 这个漏洞的意义在于：对 那些一般以低权限运行的企业用户具备较大的威胁，攻击程序可 以因此获得高权限。 阿达的BLOG中发布了 微软官方的临时解决方案： 禁用NTVDM子 系统 注意请参阅 Microsoft知识库文章979682使用微软的自动修复解决的办法 来启用或禁用此替代方法。 1.单击开始，单击运 行，键入在打开框中，键入gpedit.msc，然后单击确 定。这将打开组策略管理器。 2.展开管理模板文件 夹，然后单击Windows组件。 3.单击应用程序兼容性 的文件夹。 4.在详细信息窗格中， 双击阻止访问16位应用程序策略设置。默认情况下，这是设置 为未配置。 5.更改策略设置启用， 然后单击确定。