 微软的Windows系统是出了名的漏洞多。如今，Windows Vista(以下简称Vista)已经发布，微软也声称Vista在安全方面有了很大的改进，会让用户数据更加安全。那么，这个新系统会不会重蹈它前辈们的覆辙，不断地暴露出各种漏洞呢? 根据Vista现有的程序设计和以往系统所暴露出的漏洞的性质，我们发现在Vista中有10个地方极可能被黑客利用，从而造成Vista安全防线的全面崩溃。 漏洞预警一：IE HTML高危溢出漏洞 类型：远程溢出漏洞 危险程度：★★★★★ 漏洞被利用后果：黑客通过IE轻松获得Vista最高权限 Internet Explorer(IE)是微软开发的网页浏览器，Vista系统中的IE7不仅仅加强了安全功能，在个人隐私保护方面也有所强化。IE7具有彻底的清除功能，而且在防止网络钓鱼方面也有很大的改进。 但是，现在互联网的安全形势越来越严峻，其中就有很多黑客布下的陷阱。在这些陷阱中，网页木马这种形式是最常见的。网页木马并非是一种全新的木马，它利用IE漏洞进行伪装，演示得和正常页面一样，可是一旦用户浏览该网页后，木马程序就会自动在系统中秘密运行了。随着Vista系统和IE7.0浏览器的逐步普及，和它们相关的漏洞也可能会大量出现。 漏洞预警二：MSN联系人拒绝服务漏洞 类型：远程代码执行漏洞 危险程度：★★★★☆ 漏洞被利用后果：黑客通过MSN漏洞导致系统崩溃或者系统被控制 最近发布的《2006年即时通讯季度平均活跃账户数排名》显示，腾讯QQ毫无悬念地排名首位。不过MSN的能量

也不可小觑，尤其是在Vista正式发布后。MSN的漏洞也层出不穷，比如“ PNG 处理中的漏洞可能允许远程执行代码 ”漏洞就是迄今为止MSN最为严重的漏洞之一。 今年年初，QQ和UC都相继出现了高危漏洞，随着MSN用户越来越多，加上微软的名头，势必会有更多的黑客高度关注MSN。这样黑客对MSN的破解分析加剧，其漏洞被发现的几率也将越来越大，各种关于MSN的病毒，比如MSN尾巴，极有可能如同QQ尾巴那样泛滥，同时利用MSN的入侵事件也会越来越多。可以预见，MSN将成为Vista庞大安全防线中的一大薄弱环节。 漏洞预警三：WMP插件缓冲区溢出漏洞 类型：任意指令执行漏洞 危险程度：★★★★☆ 漏洞被利用后果：黑客通过恶意插件控制系统 Windows Media Player(WMP)是Windows系统自带的媒体播放器。DRM是微软研发的新型拷贝防护系统，作为插件，它使用到WMP上面，会禁止用户在非高清视频输出设备上欣赏受保护的高清节目。不过Vista刚刚发布，就有人声称DRM技术已经被攻破，用户即使通过模拟接口也照样可以在Vista上观看各种高清节目。 现在就有黑客利用“ Windows媒体播放器数字权限管理加载任意网页漏洞 ”来传播网页木马。当WMP以及其他播放器播放恶意文件时，程序会弹出一个窗口说文件经过DRM加密需要验证证书，当用户点击链接下载验证证书时就会激活包含在网页中的木马程序。尽管DRM版权保护技术被攻破的消息还没有完全得到确认，不过并非没有可能。如此一来，新一轮利用多媒体文件进行木马传播的高潮又将来临。 漏洞预警四：远程桌面拒绝服务漏洞 类型：拒绝服务漏洞 危险程度：★★★★ 漏洞被利用后果：黑客绕过防火墙轻易进入系统 远程桌面是为了方便

网络管理员维护系统而推出的。网络管理员使用远程桌面连接程序连接到网络任意一台开启了远程桌面控制功能的计算机上，就好比自己操作该计算机一样，可以运行应用程序，维护数据库等。 也正因为如此，该功能推出以来，通过3389端口来进行入侵已经不是什么新鲜事。远程桌面对于任何人来说都是一个永远不会被杀毒软件查杀的后门，再加上很多用户的账户密码很简单，所以入侵更是易如反掌。所以只要远程桌面服务存在，就必将成为黑客入侵系统的主要方式之一。 漏洞预警五：Windows矢量标记语言缓冲区溢出漏洞 类型：远程溢出漏洞 危险程度：★★★★ 漏洞被利用后果：黑客通过溢出获得系统的最高权限 利用远程溢出漏洞进行入侵是如今常见的入侵方式之一，远程溢出的后果则是被黑客进行远程控制，进而会导致被黑客安装程序，或者黑客在用户的电脑中创建拥有完全用户权限的新账户等一系列高风险的后果。 很多高危的远程系统漏洞都被一些危险性极高的病毒所利用。比如2004年的“震荡波”病毒就是利用的LSASS漏洞。 影响Vista以前版本的Windows矢量标记语言缓冲区溢出漏洞已经出现，现在利用该漏洞的网页木马生成器已经随处可见。虽然受影响的系统不包括Vista系统，但是由于IE7浏览器会受到影响，Vista系统也不可避免地会受到相应的影响。