PowerPoint出现0day漏洞可能远程执行代码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_ti2020/566/2021_2022_PowerPoint_c100_566949.htm 微软安全响应中心在今天发布的安全通告(969136)中指出，存在Microsoft Office PowerPoint中的安全漏洞已经被广泛公布， 可能允许远程执行代码。Office 2000, Office XP, Office 2003 and Mac Office都存在该漏洞，而最新版本的Office 2007则不受影响。 微软安全相应中心博客目前提供了一项详细解决方案来保护你的系统环境。现在微软已经发现一些不同的攻击文件被使用，但是他们仅被使用在特定目标的攻击，所以受影响的客户数量不大。以下的图表用来展示此类的攻击如何进行： 通常这些文件看起来没有什么问题，当打开之后会在毫无通知的情况下在后台运行恶意软件。以下的两个例子是此类幻灯片的第一页： 另外微软还发布了基因码检测（generic signature）信息来帮助用户对付这些漏洞，它的名称是Exploit:Win32/Apptom.gen，通常这些攻击文件将阻止用户打开Windows Live OneCare或者Forefront Client Security软件。 这些包含恶意软件的PPT文件一旦被打开立即向电脑投下恶意软件，以下的截图显示了恶意文档被执行之后的进程活动情况： 发现的恶意软件类型主要有： Fssm32.exe : TrojanDropper:Win32/Apptom.A Setup.exe: TrojanDropper:Win32/Apptom.B IEUpd.exe: Trojan:Win32/Cryptrun.A 目前这些攻击性文件已经被递交到VirusTotal网站，相信反病毒软件将很快做出反应，以下是这三个恶意软件的SHA1值和MD5： 通常情况下在打开不明来源的附件时要小心谨慎，同时要确保反病毒软件病毒库的

更新。微软将很快发布相应的安全补丁。 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