揭秘WindowsServer2008蓝屏漏洞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__E6_8F_AD_E7_A7_98Wind_c100_644209.htm 蓝屏漏洞威胁的是服务器操作系统WindowsServer2008，这意味着如果WindowsServer2008蓝屏，将导致服务器停止服务……目前，漏洞的利用代码还限制在小范围内，不过漏洞攻击工具却已经研制出来了，现在为大家揭秘蓝屏漏洞的利用过程。 问题： Windows Server 2008蓝屏漏洞 危害： 服务器出现蓝屏停止服务 危机：服务器的蓝屏隐痛 我是安天实验室的苗得雨，我下面给大家说的就是蓝屏漏洞。蓝屏漏洞的正式名称是SMBv2漏洞，到截稿为止该漏洞还没有补丁(预计10月第二个星期出补丁)。蓝屏漏洞的危害到底有多大？对我们普通网民会带来危害吗？蓝屏漏洞主要威胁的是使用WindowsServer2008的服务器，对 Vista系统也有一定的影响。不过现在的黑客都变得务实起来，不会对市场份额尴尬的Vista系统感兴趣。 使用WindowsServer2008作为服务器操作系统的，是邮件服务器、网站服务器、数据服务器、域名服务器等。一旦服务器蓝屏了，管理员很可能不会第一时间知道因为很多服务器都没有配专用的显示器，服务器就会在一段时间内停止服务。 如果是网站服务器停止服务了，服务器上的所有网站都无法访问；如果是邮件服务器停止服务了，邮件就不能中转发送；如果是数据服务器停止服务了，可能会导致数据支持的系统崩溃，例如网游、网银等系统；如果是域名服务器停止服务了，“ 断网门 ”可能再次上演。 2007年，微软发布了替换WindowsServer2003的新一代服务器操作系

统WindowsServer2008，该系统支持多核处理器，拥有64-bit技术、虚拟化以及优化的电源管理等功能，吸引了许多企业用户将服务器操作系统更换为该系统。 据市场调研机构Gartner提供的数据显示，在2007年全球发货的服务器中，Windows服务器的份额已经增长到66.8%，其中 WindowsServer2008占了主流。在2008年~2009年，WindowsServer2008成为微软的主打产品之一，份额呈现上升趋势。根据以上数据测算，全球大约有五分之一的服务器使用的操作系统是WindowsServer2008。 原理：SMB溢出 这次导致蓝屏漏洞出现的原因，是一个名为SRV2.SYS的驱动文件不能正确地处理畸形数据结构请求。如果黑客恶意构造一个恶意畸形的数据报文发送给安装有WindowsServer2008的服务器，那么就会触发越界内存引用行为，让黑客可以执行任意的恶意代码(图1)。 编注：SMB(Server MessageBlock，又称CommonInternetFileSystem)是由微软开发的一种软件程序级的网络传输协议，主要作用是使一个网络上的机器共享计算机文件、打印机、串行端口和通讯等资源。它也提供认证的进程间通信机能。它主要用在装有MicrosoftWindows的机器上，这样的机器被称为MicrosoftWindowsNetwork。SMBv2是SMB协议的最新升级版。 做一个形象的比喻，这就如同一座大桥的检查站一样，检查人员只根据卡车上标注的吨位来估算卡车能否通过这座桥，而事实上黑客可以让一辆超载的卡车同样标注上合格的吨位通过检查站。由于没有做真正的称重，检查人员只凭借标注吨位来识别，最终导致超载的卡车危及大桥安全，导致桥毁车亡。 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