网络已出现针对IIS漏洞攻击计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E7_BD_91_E7_BB_9C_E5_B7_B2_E5_c98_644438.htm 微软更新安全报告，指出已发现针对Internet Information Services（IIS）FTP服务安全漏洞的攻击。而且微软原本以为该漏洞仅影响IIS 5.0、IIS 5.1及IIS 6.0，但最新的报告则显示IIS 7.0亦无法幸免。这是一个FTP服务堆栈溢出漏洞，若FTP服务器允许未被授权的使用者登入而且可建立一个很长且特制的目录，就可能触发该漏洞，让黑客可以执行程序或进行阻断式服务攻击。 早在一周前专门搜集攻击程序的Milw0rm网站就出现针对该漏洞的攻击程序，首只攻击程序主要锁定Windows 2000服务器上所执行的IIS 5.0。而上周Milw0rm站上再度出现锁定其他平台进行阻断式服务攻击的概念性验证程序，包括Windows XP上的IIS 5.1、Windows 2003所使用的IIS 6.0，以及Windows Vista及Windows Server 2008平台上的IIS 7.0都受到波及。 微软安全响应中心Alan Wallace上周证实已发现针对IIS FTP漏洞的有限攻击。来源：考试大 不过，微软IIS团队成员Wade Hilmo则表示，上周新出现的概念性验证程序是锁定另一个IIS FTP服务漏洞，只是它与首个出现的漏洞有相同的影响，而解决方法亦类似。 Hilmo指出，两个概念性验证程序皆是由同一个研究人员所揭露，而且该研究人员都是选择直接向大众发表，而未先知会微软。 IIS与FTP的版本别有些不一致而混淆了不少人。通常IIS与FTP版本是相对应的，但IIS 6.0及IIS 7.0则例外皆采用FTP 6.0版本，而且微软额外针对Vista及Windows Server 2008平台供应FTP 7.0扩充组件，Hilmo说明，目前的调

查显示FTP 7.0及Windows 7与Windows 2008 R2所采用的FTP 7.5是不受影响的。 该版本别的设计也导致微软安全响应中心初期宣布IIS 7.0并未受到影响。 在更新程序尚未出炉前，微软建议用户可以关闭FTP服务，或是避免利用NTFS ACLs建立新的目录，而且也不要让不明的用户透过IIS设计写入数据。 微软即将于本周二（9/8）进行例行性更新，但外界认为微软应该来不及于此次更新修补该漏洞。 编辑特别推荐: 三级网络考前密卷选择题 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