WindowsFTP客户端多个远程溢出漏洞 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/460/2021_2022_WindowsFTP_c100_460824.htm 发布日期：2007-11-27 更新日期：2007-11-29 受影响系统：Microsoft Windows XP Microsoft Windows 2000SP4 Microsoft Windows 2000 Server SP4 描述：Windows系统自带的FTP客户端实现上存在缓冲区溢出漏洞，远程攻击者可能利用此漏洞控制客户端。 Windows操作系统所捆绑的FTP客户端没有正确地验证mget、dir、user、password、ls等命令，如果用户使用FTP客户端连接到了FTP服务器上带有超长文件夹名或文件名的目录并发布了上述命令的话，就可以触发缓冲区溢出，导致拒绝服务或执行任意指令。但这个漏洞较难利用，因为需要社会工程学且必须以有漏洞命令参数的形式注入shellcode. 测试方法： 警 告 以下程序（方法）可能带有攻击性，仅供安全研究与教学之用。使用者风险自负！http://www.xdisclose.com/poc/mget.bat.txt http://www.xdisclose.com/poc/username.bat.txt http://www.xdisclose.com/poc/directory.bat.txt http://www.xdisclose.com/poc/list.bat.txt 建议： 目前厂商还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页以获取最新版本：http://www.microsoft.com/technet/security/ 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