IOSLPD远程缓冲区溢出漏洞思科认证 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_IOSLPD_E8_BF_9C_E7_c101_644159.htm Cisco IOS是Cisco网络设备中所使用的操作系统。 Cisco IOS的LPD服务在处理超长的设备名时存在缓冲区溢出漏洞，远程攻击者可能利用此漏洞控制设备或导致设备拒绝服务。百考试题－全国最大教育类网站(100test.com) 行式打印机服务（LPD）用于在Cisco IOS中提供打印服务。如果IOS中配置了LPD守护程序的话，该服务会监听于默认的LPD端口TCP 515。如果任何非515的源TCP端口进行连接时，就会显示以下错误： $ telnet 172.30.3.101 515 Trying 172.30.3.101... Connected to 172.30.3.101 (172.30.3.101). Escape character is ^]. hostname_of_the_router: /usr/lib/lpd: Malformed from address 如果主机名大于等于99个字符的话，就会由于调用sprintf()函数而导致溢出。尽管技术上是栈溢出，但由于IOS为进程栈分配堆内存，因此所覆盖的内存实际为堆。由于堆内存用作了栈，在出现溢出时主机名可以覆盖存储在字符缓冲区开始之前的返回地址，但由于某些原因在缓冲区到达堆块边界处的red zone之前不会出现崩溃，因此在出现崩溃和路由器重启后，内存dump显示的是堆破坏。 必须要控制主机名才能利用这个漏洞。如果设备上在运行SNMP且知道rw团体字符串（通常为默认值private），就可以如下设置主机名： $ snmpset -Os -c private -v 1 10.0.0.1 system.sysName.0 s long_hostname 链接 ：http://www.irmplc.com/index.php/155-Advisory-024 http://www.cisco.com/warp/public/707/cisco-sr-20071010-lpd.shtm

l http://secunia.com/advisories/27169/ * 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