

微软Windows2000本地安全策略可被破坏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\\_\\_E5\\_BE\\_AE\\_](https://www.100test.com/kao_ti2020/644/2021_2022__E5_BE_AE_)

[E8\\_BD\\_AFWind\\_c100\\_644517.htm](https://www.100test.com/kao_ti2020/644/2021_2022__E5_BE_AE_E8_BD_AFWind_c100_644517.htm) 受影响系统：Microsoft Windows NT 2000 不受影响系统：Microsoft Windows NT 4.0 Microsoft Windows NT 2000 Datacenter 描述：NSFOCUS ID：795 BUGTRAQ ID：1613 CVE/CAN ID：CVE-2000-0771 恶意用户可能破坏一台Windows 2000机器上的本地安全策略，从而使得它拒绝提供网络服务。本地安全策略负责确定：用来鉴别登录企图的受信任域. 谁可以存取该系统以及如何存取(谁可以存取该网络服务以及如何交互式地存取). 谁被分配了特权. 该实施什么样的安全审核. 默认的内存配额的建立。这可以控制单个用户可以使用的分页及非分页内存池的大小。如果Windows 2000客户端的本地安全策略被成功地破坏掉，则用户将无法执行登录域、从服务器上下载文件、共享文件等操作。如果域控制器上的本地安全策略被成功破坏掉，则整个域中的网络服务都被去除了。当本地安全策略被破坏时，唯一的解决办法是从备份中恢复成众所周知的配置。发动攻击的用户并不要求是已鉴权用户。任何远程或本地用户只要能建立RPC连接并遵循一系列特定的步骤就能利用这个漏洞。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](http://www.100test.com)