新黑客技巧可能导致Oracle发生泄露 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/220/2021_2022__E6_96_B0_E9_BB_91_E5_AE_A2_E6_c67_220309.htm 一名安全研究人员警告说，一种新的攻击技巧增加了Oracle数据库软件中常见漏洞的风险。 过去，人们一般认为攻击者需要取得数据库的高级权限才能利用所谓的PL SQL注入脆弱性。不过NGS Software信息安全专家David Litchfield周四在Black Hat DC大会上说，一种新的攻击技巧改变了这一事实。“ 攻击者只要具备最低权限，就可以用这种技巧完全控制数据库服务器， ”Litchfield在接受访问时说：“ 你可以用它来入侵许多你过去认为并不重要的漏洞。 ”长期研究Oracle软件的Litchfied于上周在Black Hat DC大会上公开发表一篇论文，详细讨论这种他称为“ 指针注入 ”（cursor injection）的技巧，利用该技巧的攻击代码实例已经出现，Litchfield说。 Oracle也发出声明指出，该公司已注意到这种新的攻击手段。“ NGS Software的‘ Cursor Injection ’论文说明了一种可能协助攻击者利用SQL注入脆弱性的技巧， ”这家数据库开发商称。Oracle强烈要求客户安装它提供的补丁修复已知的漏洞。 过去，PL SQL注入漏洞通常要求攻击者具有数据库的“ 建立程序 ”(create procedure)权限，大多数用户都没有这种权限。而使用指针注入技巧，任何人只要连接数据库就可以利用这种漏洞，Litchfield说。“ 它通过将预先编译的指针注入易受攻击的PL SQL对象中达到攻击目的， ”Litchfield在论文中指出，“ 本研究目的在于说明，所有SQL注入漏洞不需要任何系统权限（‘ 建立会话 ’权限除外）就可以加以充分利用。 ”以后，Oracle不应再把权

限要求作为延迟修复PL SQL漏洞的理由，Litchfield说。Oracle的客户可能会因延迟安装补丁而身陷危险之中，他说。“ 现在，不给这个特殊的漏洞打补丁的借口已经不再存在，”Litchfield说。 尽管Litchfield认为他的发现增加了许多Oracle脆弱性的严重程度，但另一位著名数据库安全研究员并不同意他的观点。“ Davids指出的例子仅适用于某名用户在一个高权限的账户中使用特殊的权限和动态语句建立一个易受攻击的数据包的情况，”管理德国Red Database Security公司的Alexander Kornbrust指出：“ 我在审查PL SQL源代码时从未发现这种情况，而且我还检查了许多用户和公司的PL SQL源代码。”Oracle几年来常和安全研究人员发生摩擦。不过，公司已经做出改变，愿意诚实面对产品安全流程中存在的问题。一月，Oracle开始提前通知每季的补丁发布情况。去年十月，该公司首次在通报中加入严重等级。 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