访问Oracle数据库时如何限制绕过漏洞 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/143/2021_2022__E8_AE_BF_E9_97_AEOrac_c102_143386.htm 导 读 Oracle 9.2.0.0到10.2.0.3版本允许在基表中仅有SELECT权限的用户通过特制的视图插入/更新/删除数据，成功利用这个漏洞的低权限用户可以通过创建特制的视图导致插入、更新和删除数据。 受影响系统：Oracle Database 9.2.0.0 - 10.2.0.3 描 述： BUGTRAQ ID: 17426 Oracle是大型的商业数据库系统。Oracle 9.2.0.0到10.2.0.3版本允许在基表中仅有SELECT权限的用户通过特制的视图插入/更新/删除数据，成功利用这个漏洞的低权限用户可以通过创建特制的视图导致插入、更新和删除数据。 这个漏洞对Oracle数据词典的影响较低，因为大多数词典表没有primary key，而利用这个漏洞必须primary key。 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！ 假设用户dbsnmp仅有SELECT ANY DICTIONARY权限，无法更新数据词典中的表格。 C:\>sqlplus dbsnmp/dbsnmp SQL*Plus: Release 10.1.0.4.0 - Production on Thu Apr 8 19:20:27 2006 Copyright (c) 1982, 2005, Oracle. All rights reserved. Connected to: Oracle Database 10g Enterprise Edition Release 10.1.0.4.0- Production With the Partitioning, OLAP and Data Mining options SQL> 0select * from v$version. BANNER Oracle Database 10g Enterprise Edition Release 10.1.0.4.0 - Prod PL/SQL Release 10.1.0.4.0 - Production CORE 10.1.0.4.0 Production TNS for 32-bit Windows: Version 10.1.0.4.0 - Production NLSRTL Version 10.1.0.4.0 - Production SQL> -- 无法

从数据词典删除数据（正常） SQL> 0delete from sys.registry$. 0delete from sys.registry$ * ERROR at line 1: ORA-01031: insufficient privileges SQL> -- 创建特制的自定义视图 SQL> create or replace view e as 0select [...censored...]. View created. SQL> -- 通过视图丢弃数据!!! ==> 安全漏洞 !!! SQL> 0delete from e. 17 rows 0deleted.建议，临时解决方法: 如果您不能立刻安装补丁或者升级，NSFOCUS建议您采取以下措施以降低威胁： * 过滤9i到10g R1的连接角色，删除CREATE VIEW（以及CREATE DATABASE LINK等）权限。 * 从基表删除primary key。请注意这可能导致性能和完整性问题。 厂商补丁： Oracle 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。