记 Oracle 一次高危漏洞补丁修复过程

一、概述

本次技术讨论暂不评价微博好坏，不过本人得知这次 BUG 确实来源于微博，截图如下：

Dear Gokhan
kindly please notice the followings because in the following example a user just with grant select can modify a table :

1- create user user1 identified by 123;
2- grant create session,create table to user1;
3- grant select on scott.emp to user1;
4- in sqlplus conn user1/123
5- select ename,sal from scott.emp where ename='ALLEN';
ENAME SAL

ALLEN 3600

1 row selected

6- update scott.emp set sal=1000 where ename='ALLEN';
error at line 1:
ORA-01031: insufficient privileges

now notice the following:
update (with tmp as (select * from scott.emp) select * from tmp) set sal=1000 where ename='ALLEN';

1 row updated.

sql> commit;
commit completed.

and the last:
select ename,sal from scott.emp where ename='ALLEN';
ENAME SAL

ALLEN 1000

由上图可知，在版本 11.2.0.4 中用户无 update 权限，可以通过 with as 绕过执行 DML 操作。经过几个版本测试，发现 11.2.0.1/12.1.0 也有这样的问题，10g 无此问题。

二、 解决过程

当以为这是一个 Oracle 新版本中的新 BUG 时，恩墨发表了一篇《【云和恩墨】Oracle 数据库高危漏洞警告》，借此参考，我从官网下载 PSU 补丁，安装并测试，安装完成后此高危漏洞得到修复。

首先，再次测试一下，该版本下执行 update 语句。

```
[oracle@ora11 soft]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.4.0 Production on Thu May 14 08:57:43 2015

Copyright (c) 1982, 2013, Oracle.  All rights reserved.
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> create user test identified by test;
User created.
SQL> grant create session,connect to test;
Grant succeeded.
SQL> grant select on scott.emp to test;
Grant succeeded.
SQL> conn test/test
Connected.
SQL> select * from scott.emp;
 EMPNO ENAME      JOB              MGR HIREDATE                 SAL    COMM    DEPTNO
------ ---------- --------- ------- ------------------- ---------- ----- -------
  7369 SMITH      CLERK           7902 1980-12-17 00:00:00        800                20
  7499 ALLEN      SALESMAN        7698 1981-02-20 00:00:00       1600     300        30
  7521 WARD       SALESMAN        7698 1981-02-22 00:00:00       1250     500        30
  7566 JONES      MANAGER         7839 1981-04-02 00:00:00       2975                20
  7654 MARTIN     SALESMAN        7698 1981-09-28 00:00:00       1250    1400        30
  7698 BLAKE      MANAGER         7839 1981-05-01 00:00:00       2850                30
  7782 CLARK      MANAGER         7839 1981-06-09 00:00:00       2450                10
  7788 SCOTT      ANALYST         7566 1987-04-19 00:00:00       3000                20
  7839 KING       PRESIDENT            1981-11-17 00:00:00       5000                10
  7844 TURNER     SALESMAN        7698 1981-09-08 00:00:00       1500        0       30
  7876 ADAMS      CLERK           7788 1987-05-23 00:00:00       1100                20
  7900 JAMES      CLERK           7698 1981-12-03 00:00:00        950                30
  7902 FORD       ANALYST         7566 1981-12-03 00:00:00       3000                20
  7934 MILLER     CLERK           7782 1982-01-23 00:00:00       1300                10
SQL> update scott.emp set sal=1699 where ename='ALLEN';
update scott.emp set sal=1699 where ename='ALLEN'
                  *
ERROR at line 1:
ORA-01031: insufficient privileges
SQL> update (with temp as (select * from scott.emp) select * from temp) set sal=1699 where ename='ALLEN';

1 row updated.
SQL> commit;
```

```
Commit complete.
```

确认该漏洞存在，下面我们开始为该版本数据库打最新 PSU 补丁。
根据这篇文章《Oracle Critical Patch Update Advisory - July 2014》，找到受影响的数据库及版本，顺便简单介绍一下怎么通过 Oracle 官网查找补丁。

Affected Products and Components

Security vulnerabilities addressed by this Critical Patch Update affect the products listed in the categories below. The product area of the patches for the listed versions is shown in the Patch Availability column corresponding to the specified Products and Versions column. Please click on the link in the Patch Availability column below or in the Patch Availability Table to access the documentation for those patches.

The list of affected product releases and versions that are in Premier Support or Extended Support, under the Oracle Lifetime Support Policy is as follows:

Affected Products and Versions	Patch Availability
Oracle Database 11*g* Release 1, version 11.1.0.7	Database
Oracle Database 11*g* Release 2, versions 11.2.0.3, 11.2.0.4	Database
Oracle Database 12*c* Release 1, version 12.1.0.1	Database
Oracle Fusion Middleware 11*g* Release 1, version 11.1.1.7	Fusion Middleware
Oracle Fusion Middleware 12*c* Release 1, version 12.1.2.0	Fusion Middleware
Oracle Fusion Applications, versions 11.1.2 through 11.1.8	Fusion Applications
Oracle Glassfish Server, versions 2.1.1, 3.0.1, 3.1.2	Fusion Middleware
Oracle Traffic Director, version 11.1.1.7.0	Fusion Middleware

点击 Database，打开文档 ID 1666884.1，选择关于该版本相关补丁，当然我们可以选择最新补丁，在这里我根据其 Table，选择了补丁 Patch 18522509

Table 10 Patch Availability for Oracle Database 11.2.0.4

Product Home	Patch	Advisory Number	Comments
Oracle Database home	Database 11.2.0.4 SPU Patch 18681862, or Database 11.2.0.4.3 PSU Patch 18522509, or GI 11.2.0.4.3 PSU Patch 18706472, or Microsoft Windows (32-Bit) & x64 (64-Bit) BP 7 Patch 18842982, or later; Quarterly Database Patch for Exadata (July 2014) 11.2.0.4.9 BP Patch 18840215, or Quarterly Full Stack download for Exadata (July 2014) BP Patch 19067488	CVE-2014-4236, CVE-2014-4237, CVE-2014-4245	

由于该补丁非最新补丁，在你点击该补丁号打开后，Oracle 会提醒你，此补丁程序已被取代。如下图所示，我们可以选择最新补丁，20299013 点击下载。

⚠此补丁程序已被取代。

原因

Patch 19121551 is superset of Patch 18522509

注释

This patch was originally replaced by patch 19121551. The most recent replacement for this patch is 20299013.

替换选项(包含或取代此补丁程序的已知补丁程序或补丁程序集)

19121551	DATABASE PATCH SET UPDATE 11.2.0.4.4 (INCLUDES CPUOCT2014)	补丁程序
20299013	DATABASE PATCH SET UPDATE 11.2.0.4.6 (INCLUDES CPUAPR2015)	补丁程序

下载完成后，讲补丁程序上传至需打补丁的数据库服务器，解压，阅读相关文件 README.html。
其中有一先决条件

2.1 OPatch Utility

You must use the OPatch utility version 11.2.0.3.6 or later to apply this patch. Oracle recommends that you use the latest released OPatch version for 11.2, which is available for download from My Oracle Support patch 6880880 by selecting the 11.2.0.0.0 release.

For information about OPatch documentation, including any known issues, see My Oracle Support Document 293369.1 *OPatch documentation list*.

查看该数据库 OPatch 版本

```
[oracle@ora11 ocm]$ $ORACLE_HOME/OPatch/opatch lsinventory -detail -oh $ORACLE_HOME
Oracle Interim Patch Installer version 11.2.0.3.4
Copyright (c) 2012, Oracle Corporation.  All rights reserved.


Oracle Home           : /oracle/app/oracle/product/11.2.0
Central Inventory : /oracle/app/oraInventory
   from               : /oracle/app/oracle/product/11.2.0/oraInst.loc
OPatch version    : 11.2.0.3.4
OUI version           : 11.2.0.4.0
```

此 PUS 补丁要求 OPatch 版本必须 11.2.0.3.6 以上，不信邪，那我们执行以下试试。

```
[oracle@ora11 20299013]$ opatch apply
Oracle Interim Patch Installer version 11.2.0.3.4
Copyright (c) 2012, Oracle Corporation.  All rights reserved.


Oracle Home           : /oracle/app/oracle/product/11.2.0
Central Inventory : /oracle/app/oraInventory
```

```
        from                : /oracle/app/oracle/product/11.2.0/oraInst.loc
    OPatch version      : 11.2.0.3.4
    OUI version         : 11.2.0.4.0
    Log file location : /oracle/app/oracle/product/11.2.0/cfgtoollogs/opatch/opatch2015-05-14_10-20-22AM_1.log

    Verifying environment and performing prerequisite checks...
    Prerequisite check "CheckMinimumOPatchVersion" failed.
    The details are:


    The OPatch being used has version 11.2.0.3.4 while the following patch(es) require higher versions:
    Patch 17478514 requires OPatch version 11.2.0.3.5.
    Patch 18031668 requires OPatch version 11.2.0.3.5.
    Patch 18522509 requires OPatch version 11.2.0.3.5.
    Patch 19121551 requires OPatch version 11.2.0.3.5.
    Patch 19769489 requires OPatch version 11.2.0.3.5.
    Patch 20299013 requires OPatch version 11.2.0.3.5.
    Please download latest OPatch from My Oracle Support.

    UtilSession failed: Prerequisite check "CheckMinimumOPatchVersion" failed.
    Log file location: /oracle/app/oracle/product/11.2.0/cfgtoollogs/opatch/opatch2015-05-14_10-20-22AM_1.log

    OPatch failed with error code 73
[oracle@ora11 20299013]$
```

好了，我们根据补丁包中 README.html，链接点击下载 OPatch 补丁（注意，选择好数据库版本、操作系统版本）patch 6880880。
上传给 OPatch 补丁，我们准备开始执行补丁安装。
备份原 OPatch 目录，解压新的 OPatch 目录，并拷贝。

```
    [oracle@ora11 soft]$ unzip p6880880_112000_Linux-x86-64.zip
[oracle@ora11 soft]$ cp -r OPatch $ORACLE_HOME
--查看 OPatch 版本
[oracle@ora11 OPatch]$ ./opatch lsinventory
    Oracle Interim Patch Installer version 11.2.0.3.10
    Copyright (c) 2015, Oracle Corporation.  All rights reserved.
    Oracle Home           : /oracle/app/oracle/product/11.2.0
    Central Inventory : /oracle/app/oraInventory
        from              : /oracle/app/oracle/product/11.2.0/oraInst.loc
    OPatch version      : 11.2.0.3.10
     OUI version         : 11.2.0.4.0
     ……..
```

下面执行 PUS 补丁程序
关于监听、数据库

```
shutdown immediate| lsnrctl stop
```

解压 PSU，进入目录，执行以下命令

```
unzip p20299013_112040_Linux-x86-64.zip
cd 20299013
opatch apply
```

执行完成后，启动数据库，执行 SQL 脚本，到此，PSU 补丁打完。

```
    cd $ORACLE_HOME/rdbms/admin
    sqlplus /nolog
    SQL> CONNECT / AS SYSDBA
    SQL> STARTUP
    SQL> @catbundle.sql psu apply
```

查看：

```
    [oracle@ora11 admin]$ opatch    lsinventory
    Oracle Interim Patch Installer version 11.2.0.3.10
    Copyright (c) 2015, Oracle Corporation.    All rights reserved.
    Oracle Home            : /oracle/app/oracle/product/11.2.0
    Central Inventory : /oracle/app/oraInventory
        from                 : /oracle/app/oracle/product/11.2.0/oraInst.loc
    OPatch version       : 11.2.0.3.10
    OUI version            : 11.2.0.4.0
    Log                              file                              location                          :
/oracle/app/oracle/product/11.2.0/cfgtoollogs/opatch/opatch2015-05-14_10-50-38AM_1.log

    Lsinventory                 Output                 file                 location                  :
/oracle/app/oracle/product/11.2.0/cfgtoollogs/opatch/lsinv/lsinventory2015-05-14_10-50-38AM.txt

    --------------------------------------------------------------------------------
    Local Machine Information::
    Hostname: ora11
    ARU platform id: 226
    ARU platform description:: Linux x86-64

    Installed Top-level Products (1):
```

```
Oracle Database 11g                                                    11.2.0.4.0
There are 1 products installed in this Oracle Home.


Interim patches (1) :

Patch    20299013         : applied on Thu May 14 10:47:37 CST 2015
Unique Patch ID:    18573940
Patch description:    "Database Patch Set Update : 11.2.0.4.6 (20299013)"
Created on 4 Mar 2015, 02:27:44 hrs PST8PDT
  ....................
```

重新验证 Oracle 数据库高危漏洞，Oracle11.2.0.4 版本已修复。

```
SQL> conn test/test
Connected.
SQL> update (with temp as (select * from scott.emp) select * from temp) set sal=1600 where ename='ALLEN';
update (with temp as (select * from scott.emp) select * from temp) set sal=1600 where ename='ALLEN'
                                                                    *
ERROR at line 1:
ORA-01031: insufficient privileges
```

三、总结

当看到这个漏洞时，知道它的危险性，也觉得奇怪，谁没事会尝试使用这样的命令去更新，很佩服发现该漏洞的人员，以及在漏洞出现后恩墨及时更新说明（当然，也许只是我孤陋寡闻）。在本人目光有限的情况下，知道有一些公司以及数据库管理人员对 Oracle 发布的一些补丁并为及时更新，当然也有各种缘由。数据库存储数据，它的重要性不言而喻，在我们认真学习技术的同时也应该多关注 Oracle 方面发布的相关公告、补丁程序等，善于利用 Oracle 网站、MOS，将会助你更好的学习、工作。还锻炼英语，不错的选择。

四、参考文档：

http://mp.weixin.qq.com/s?__biz=MjM5MzExMTU2OQ==&mid=205651373&idx=1&sn=4fcd886575af062c3c5814e73541cb26&scene=5#rd
【云和恩墨】Oracle 数据库高危漏洞警告！

网名：文盲筱烨
IT 技术、跑步爱好者
Oracle10g OCM 、SDOUG 成员（一个朝气年轻的组织）
邮箱：longzhimeng99@sina.com
博客：http://blog.itpub.net/29487349/