

Oracle Security

Spring 2018



DBA Threat Assessment

Dan Morgan

Anatomy of an IT Terrorist Attack (1:7)

- Oracle releases a new security patch
 - Attackers download it within minutes
 - Attackers read the list of weaknesses
 - Attackers know they have weeks/months before Oracle's customers will apply the patch
-
- I am going to teach everyone here how to attack any Oracle Database
 - With no escalated privileges
 - Without any tools or techniques such as SQL Injection
 - And with one only one SQL statement and one line of code
 - You have an ethical and moral responsibility to use this information only for the purpose of helping your organization understand the risk they are taking by not investing in data security

Anatomy of an IT Terrorist Attack (2:7)

Document Display

Give Feedback...

Search: database security patch

Back to Results

- Agile Server Not Starting Fully After Database Security Patch 21523375 (2074804.1)
- Security Patch Update April 2017 Database Known Issues (2229042.1)
- Security Patch Update July 2017 Database Known Issues (2264640.1)
- Security Patch Update October 2017 (11.2.0.4.171017) Database Known Issues (2297788.1)
- Potential Impact of Installing Oracle Database Security Patches on Servers running OCNCC (1559390.1)
- Database Security Patching from 12.1.0.1 onwards (1581950.1)
- FAQ - SES Mandatory Software Patches And Security Patch Certification Information (2204694.1)
- Information Center: Patching and Maintaining Database Security Products (1548957.2)
- All About Security: User, Privilege, Role, SYSDBA, O/S Authentication, Audit, Encryption, OLS, Database Vault, Audit Vault (207959.1)
- Security Checklist: 10 Basic Steps to Make Your Database Secure from Attacks (1545816.1)

Load More...

Back to Results

PURPOSE

This document lists the known issues for Oracle Database Security Patch Update (11.2.0.4.171017) dated October 17, 2017. These known issues are in addition to the issues listed in the individual READMEs.

SCOPE

The document is for Database Administrators and/or others tasked with Quarterly Security Patching.

DETAILS

Patch 26474853 - Security Patch Update October 2017 (11.2.0.4.171017) Database Known Issues

For CPUOct2017

My Oracle Support Document ID: 2297788.1

Released: October 17, 2017

This document lists the known issues for Oracle Database Security Patch Update dated October 2017 - 11.2.0.4.171017 (aka patch 26474853). These known issues are in addition to the issues listed in the individual CPUOct2017 READMEs.

This document includes the following sections:

- Section 1. "Known Issues"
- Section 2. "Modification History"
- Section 3. "Documentation Accessibility"

1 Known Issues

Was this document helpful?

- Yes
- No

Document Details

Type: REFERENCE
Status: PUBLISHED
Last Major Update: Oct 30, 2017
Last Update: Oct 30, 2017

Information Centers

No Information Center available for this document.

Document References



No References available for this document.

Recently Viewed

- Secure Configuration for Oracle E-Business Suite Release 12.1 [403537.1]
- Secure Configuration Guide for Oracle E-Business Suite 11i [189367.1]
- Can The QWADIR Schema Be

Anatomy of an IT Terrorist Attack (3:7)

Patch Details

  **Patch 26474853: DATABASE SECURITY PATCH UPDATE 11.2.0.4.171017**

Last Updated Oct 30, 2017 6:20 PM (5+ months ago)

Product	Oracle Database - Enterprise Edition (More...)	Size	19.4 MB
Release	Oracle 11.2.0.4.0	Download Access	Software
Platform	IBM: Linux on System z	Classification	Security
		Patch Tag	All Database

Recommendations / Certifications

Recommended for Oracle Database 11.2.0.4.0

Bugs Resolved by This Patch

13944971	Fix for Bug 13944971
16450169	Fix for Bug 16450169
16524926	APEX: ORA-1031 WITH ORACLE MULTIMEDIA AND REALM PROTECTED DB SCHEMA
16721594	Fix for Bug 16721594
17006570	Fix for Bug 17006570
17088068	Fix for Bug 17088068
17343514	REMOVE JAVA FROM CATBUNDLE
17551063	Fix for Bug 17551063
17551709	DATABASE SECURITY PATCH UPDATE 11.2.0.4.0 (CPUJAN2014)
17600719	DBMS_UTILITY.INVALIDATE ORA-3113 ORA-7445 CORE DUMP [OPIGLN]

[Open Readme to View all Bugs](#)

183.6.26 INVALIDATE Procedure

This procedure invalidates a database object and (optionally) modifies its PL/SQL compiler parameter settings. It also invalidates any objects that (directly or indirectly) depend on the object being invalidated.

Syntax

```
DBMS_UTILITY.INVALIDATE (  
    p_object_id          NUMBER,  
    p_plsql_object_settings VARCHAR2 DEFAULT NULL,  
    p_option_flags       PLS_INTEGER DEFAULT 0);
```

Anatomy of an IT Terrorist Attack (5:7)

```
sqlplus.exe

SQL*Plus: Release 12.2.0.1.0 Production on Fri Apr 13 08:12:31 2018

Copyright (c) 1982, 2016, Oracle. All rights reserved.

Enter user-name: / as sysdba

Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production

Session altered.

Session altered.

SQL> SELECT grantee FROM dba_tab_privs WHERE table_name = 'DBMS_UTILITY' ORDER BY 1;

GRANTEE
-----
DBSFUSER
DVSYS
GSMADMIN_INTERNAL
ORDSYS
PUBLIC
WMSYS

6 rows selected.
```

Anatomy of an IT Terrorist Attack (6:7)

```
SQL> CREATE TABLE test (  
2 testcol VARCHAR2(20));
```

Table created.

```
SQL> CREATE OR REPLACE PROCEDURE testproc IS  
2 i PLS_INTEGER;  
3 BEGIN  
4 SELECT COUNT(*)  
5 INTO i  
6 FROM test;  
7 END testproc;  
8 /
```

SP2-0804: Procedure created with compilation warnings

```
SQL> SELECT object_id, object_name, object_type  
2 FROM user_objects  
3 WHERE object_name = 'TESTPROC';
```

OBJECT_ID	OBJECT_NAME	OBJECT_TYPE
88434	TESTPROC	PROCEDURE

```
SQL> SELECT object_id FROM user_objects WHERE object_name = 'TESTPROC';
```

```
OBJECT_ID  
-----  
88434
```

```
SQL> exec dbms_utility.invalidate(88434);
```

PL/SQL procedure successfully completed.

```
SQL> SELECT object_id, object_name  
2 FROM user_objects  
3 WHERE status = 'INVALID';
```

OBJECT_ID	OBJECT_NAME
88434	TESTPROC

Anatomy of an IT Terrorist Attack (7:7)

- We need you to grab your keyboard and join us in the battle to protect your data, your database, your organization, and
- A data and database vulnerability audit is one place to start





Securing Database 18c with a Read Only Home

Dan Morgan

- One of the new features present in Oracle 18c in the read only Oracle home
- Why a read only home?
 - Prevents anyone from modifying files under \$ORACLE_HOME
 - /dbs (spfile)
 - /network/admin (sqlnet.ora, listener.ora, tnsnames.ora)
 - /rdbms/admin (source code for data dictionary objects, functions, packages, and procedures)
 - /sqlplus/admin (glogin.sql runs automatically with every SQL*Plus login)

```
2. Ora18Cloud
[oracle@oem13c2-demo-db18c oracle]$ ls
admin  audit  cfgtoollogs  checkpoints  diag  product
[oracle@oem13c2-demo-db18c oracle]$ cd product
[oracle@oem13c2-demo-db18c product]$ ls
18.0.0  apex  java  ords
[oracle@oem13c2-demo-db18c product]$ cd 18.0.0/
[oracle@oem13c2-demo-db18c 18.0.0]$ ls
dbhome_1
[oracle@oem13c2-demo-db18c 18.0.0]$ cd dbhome_1/
[oracle@oem13c2-demo-db18c dbhome_1]$ ls
addnode      clone  data      diagnostics  has      javavm  lib      nls      oracore    oss      precomp  relnotes  runInstaller  sqlj      ucp
apex          crs    dbjava    dmuf         hs      jdbc     log      odbc     oraInst.loc  oui     QOPatch  root.sh      schagent.conf  sqlpatch  usm
assistants   css    dbs        drdaas      install  jdk      md       olap     ord        owm     R         root.sh.bkup  sdk         sqlplus    utl
bin          ctx    deinstall dv           instantclient  jlib     mgw     OPatch   ordim      perl    racg     root.sh.old  slax         srvm       wwq
cfgtoollogs cv     demo      env.ora     inventory  ldap     network  opmn     ords       plsql   rdbms    root.sh.old.1  sqldeveloper  suptools  xdk
[oracle@oem13c2-demo-db18c dbhome_1]$
```



18c Read Only Oracle Home

By Franck Pachot | February 18, 2018 | Oracle | No Comments



This is the big new feature of Oracle 18c about database software installation. Something that was needed for decades for the ease of software deployment. [Piet de Visser](#) raised this to Oracle a long time ago, and we were talking about that recently when discussing this new excitement to deploy software in Docker containers. Docker containers are by definition immutable images. You need a Read Only Oracle Home, all the immutable files (configuration, logs, database) being in an external volume. Then, to upgrade the software, you just open this volume with an image of the new database version.

```
2. Ora18Cloud
[oracle@oem13c2-demo-db18c bin]$ pwd
/u01/app/oracle/product/18.0.0/dbhome_1/bin
[oracle@oem13c2-demo-db18c bin]$ ls -al rooh*
-rwxr-x--- 1 oracle oinstall 4631 Feb  8 08:45 roohctl
[oracle@oem13c2-demo-db18c bin]$
```

```
[oracle@oem13c2-demo-db18c bin]$ more roohctl
#!/bin/sh
#
# $Header: assistants/bin/roohctl.sh.pp /main/5 2017/09/05 01:53:02 jaikrish Exp $
#
# roohctl.sh
#
# Copyright (c) 2014, 2017, Oracle and/or its affiliates. All rights reserved.
#
# NAME
#   roohctl.sh - <one-line expansion of the name>
#
# DESCRIPTION
#   <short description of component this file declares/defines>
#
# NOTES
#   <other useful comments, qualifications, etc.>
#
# MODIFIED   (MM/DD/YY)
# mstalin    08/22/17 - 26495385 Could not get inventory location error
# mstalin    09/12/14 - Script file for roohctl
# mstalin    09/12/14 - Creation
#
#####
# Variables set by Oracle Universal Installer for dependent components.
#####
```

```
# Check if user is non-root

MYPLATFORM=`uname`

# make sure others can not read/write any files created
umask 27

# The environment variable $TWO_TASK cannot be set during the installation
unset TWO_TASK

# The environment variable $JAVA_HOME cannot be set during the installation
unset JAVA_HOME

# Basic error checking
case $OH in
  "") echo "*** ORACLE_HOME Not Set!"
      echo "    Set and export ORACLE_HOME, then re-run"
      echo "    ORACLE_HOME points to the main directory that"
      echo "    contains all Oracle products."
      exit 1;;
esac

#call platform_common script
. $ORACLE_HOME/bin/platform_common

# Check if user is non-root
if [ "$RUID" = "0" ]; then
  echo "roohctl cannot be run as root."
  exit 1;
fi

JRE_OPTIONS="${JRE_OPTIONS} -Dsun.java2d.font.DisableAlgorithmicStyles=true -DIGNORE_PREREQS=$IGNORE_PREREQS -mx128m $DEBUG_STRING"

# Set Classpath for ROOHCTL
CLASSPATH=$ROOHCTL_CLASSPATH:$ASSISTANTS_COMMON_CLASSPATH:$SHARE_CLASSPATH:$XMLPARSER_CLASSPATH:$GDK_CLASSPATH:$NETCFG_CLASSPATH:$SRVM_CLASSPATH:$INSTALLER_CLASSPATH

ARGUMENTS=""
NUMBER_OF_ARGUMENTS=$#
if [ $NUMBER_OF_ARGUMENTS -gt 0 ]; then
  ARGUMENTS=$*
fi
```

```
#####
# Run roohctl
exec $JRE_DIR/bin/java $JRE_OPTIONS -classpath $CLASSPATH oracle.assistants.roohctl.RoohCtl $ARGUMENTS
[oracle@oem13c2-demo-db18c bin]$ clear
[oracle@oem13c2-demo-db18c bin]$ pwd
/u01/app/oracle/product/18.0.0/dbhome_1/bin
[oracle@oem13c2-demo-db18c bin]$ ls -al rooh*
-rwxr-x--- 1 oracle oinstall 4631 Feb  8 08:45 roohctl
[oracle@oem13c2-demo-db18c bin]$ clear
[oracle@oem13c2-demo-db18c bin]$ more roohctl
#!/bin/sh
#
# $Header: assistants/bin/roohctl.sh.pp /main/5 2017/09/05 01:53:02 jaikrish Exp $
#
# roohctl.sh
#
# Copyright (c) 2014, 2017, Oracle and/or its affiliates. All rights reserved.
#
# NAME
#   roohctl.sh - <one-line expansion of the name>
#
# DESCRIPTION
#   <short description of component this file declares/defines>
#
# NOTES
#   <other useful comments, qualifications, etc.>
#
# MODIFIED   (MM/DD/YY)
# mstalin    08/22/17 - 26495385 Could not get inventory location error
# mstalin    09/12/14 - Script file for roohctl
# mstalin    09/12/14 - Creation
#
```

- With a Read Only Oracle Home we protect files that should be static upon install and minimize the footprint for attack to a very small number of files that must be dynamic
- To identify the new locations Oracle has created 2 new environment variables
 - Oracle Base Configuration (orabaseconfig) which exists primarily as a mapping to .ora and .dat files
 - Oracle Base Home (orabasehome) which is primarily intended as a mapping to /network/admin
- You enable a Read Only Oracle Home with `roohctl -enable` as shown below

```
[oracle@VM181 18c]$ roohctl -enable
Enabling Read-Only Oracle home.
Update orabasetab file to enable Read-Only Oracle home.
Orabasetab file has been updated successfully.
Create bootstrap directories for Read-Only Oracle home.
Bootstrap directories have been created successfully.
Bootstrap files have been processed successfully.
Read-Only Oracle home has been enabled successfully.
Check the log file /u01/app/oracle/cfgtoollogs/roohctl/roohctl-180217PM111551.log.
```

- In 12c, you can change your habits and replace all references to `${ORACLE_HOME}/dbs` with `$(oracle_base_config)/dbs` and `${ORACLE_HOME}` with `$(oracle_base_home)`. In 12c they will go to the same `ORACLE_HOME`. But you will be ready to enable ROOH in 18c

An IT Terrorist Attack (7:7)

- We need you to grab your keyboard and join us in the battle to protect your data, your database, your organization
- ROOH is a step in the right direction





SQL Rewrite Vulnerabilities

Dan Morgan

What Is A Rewrite Vulnerability?

- Rewrite occurs when the database optimizer transparently replaces executed SQL and PL/SQL with a completely different statement
- The replacement statement may improve performance
- The replacement statement may be the worst Cartesian Join you can imagine
- The replacement statement may breach your carefully crafted security
- There are three places in Oracle where rewrite occurs in most databases
 - Optimizer Rewrites
 - Enabled rewrites such as `STAR_TRANSFORMATION_ENABLED`
 - By default the Oracle database will rewrite every DML statement is processes
 - The only way you can stop this rewrite is with SQL baselines or with full hinting
 - Optimizer rewrites will never change the nature of statement and thus cannot, in and of themselves, constitute a security risk

Full Hinting (an example by Jonathan Lewis)

Consider, for example:

```
SELECT /*+ index(t1 t1_abc) index(t2 t2_abc) */ COUNT(*)
FROM t1, t2
WHERE t1.col1 = t2.col1;
```

For weeks, this may give you the plan:

```
NESTED LOOP
  table access by rowid t1
    index range scan t1_abc
  table access by rowid t2
    index range scan t2_abc
```

Then, because of changes in statistics, or init.ora parameters, or nullity of a column, or a few other situations that may have slipped my mind at the moment, this might change to:

```
HASH JOIN
  table access by rowid t2
    index range scan t2_abc
  table access by rowid t1
    index range scan t1_abc
```

Your hints are still obeyed, the plan has changed. On the other hand, if you had specified:

```
SELECT /*+ no_parallel(t1) no_parallel(t2) no_parallel_index(t1) no_parallel_index(t2)
ordered use_nl(t2) index(t1 t1_abc) index(t2 t2_abc) */ COUNT(*)
FROM t1, t2
WHERE t1.col1 = t2.col1;
```

Then I think you could be fairly confident that there was no way that Oracle could obey the hints whilst changing the access path.

Materialized View Rewrites

- Materialized View Rewrites must be authorized through DDL and instruct a query to consider using a Materialized View in place of a table
- Here are some examples of explicit MV rewrite authorizations

```
CREATE MATERIALIZED VIEW mv_rewrite
TABLESPACE uwdata
REFRESH ON DEMAND
ENABLE QUERY REWRITE
AS SELECT s.srvr_id, i.installstatus, COUNT(*)
FROM servers s, serv_inst i
WHERE s.srvr_id = i.srvr_id
GROUP BY s.srvr_id, i.installstatus;

ALTER SYSTEM SET query_rewrite_enabled = TRUE;
ALTER SYSTEM SET query_rewrite_enabled = FORCE;
ALTER SESSION SET query_rewrite_integrity = ENFORCED;
ALTER SESSION SET query_rewrite_integrity = STALE_TOLERATED;
ALTER SESSION SET query_rewrite_integrity = TRUSTED;
```

- Materialized View rewrites will never change the nature of statement and thus cannot, in and of themselves, constitute a security risk

What Is A Rewrite Vulnerability?

- But there are 3 rewrite capabilities that are far more powerful and thus far more dangers ... you need to be aware of them
 - DBMS_ADVANCED_REWRITE
 - DBMS_SQL_TRANSLATOR
 - DBMS_SQLDIAG

DBMS_ADVANCED_REWRITE

- This package contains interfaces that can be used to create, drop, and maintain functional equivalence declarations for query rewrites
- According to the Oracle docs: "To gain access to these procedures, you must connect as SYSDBA and explicitly grant execute access to the desired database administrators"

```
SQL> SELECT grantee
2 FROM dba_tab_privs
3 WHERE table_name = 'DBMS_ADVANCED_REWRITE'
4 ORDER BY 1;

no rows selected
```

- But should someone gain execute privilege on the package, for example through any one of a number of means they can do this

```
dbms_advanced_rewrite.declare_rewrite_equivalence (
name          VARCHAR2,
source_stmt   CLOB,
destination_stmt CLOB,
validate      BOOLEAN := TRUE,
rewrite_mode  VARCHAR2 := 'TEXT_MATCH');
```

and have the optimizer swap the authentic statement for one they crafted

DBMS_SQL_TRANSLATOR

- The Oracle docs state: " When translating a SQL statement or error, the translator package procedure will be invoked with the same current user and current schema as those in which the SQL statement being parsed. The owner of the translator package must be granted the TRANSLATE SQL user privilege on the current user. Additionally, the current user must be granted the EXECUTE privilege on the translator package."
- The declared business case for this package is that it can be used to intercept TransactSQL calls to an Oracle database and allow the database owner to translate those that would fail into Oracle SQL or PL/SQL

```
dbms_sql_translator.register_sql_translation(  
profile_name      IN VARCHAR2,  
sql_text         IN CLOB,  
translated_text  IN CLOB      DEFAULT NULL,  
enable          IN BOOLEAN DEFAULT TRUE);  
PRAGMA SUPPLEMENTAL_LOG_DATA(register_sql_translation, AUTO_WITH_COMMIT);
```

```
exec dbms_sql_translator.register_sql_translation(  
profile_name =>'UW_TSQLTRANS',  
sql_text =>'SELECT srvr_id INTO uwclass.tsq_target FROM uwclass.servers',  
translated_text =>'INSERT INTO uwclass.tsq_target SELECT srvr_id FROM uwclass.servers');
```


DBMS_SQLDIAG

- DBMS_SQLDIAG is part of the Oracle Diagnostic Pack and contains the procedure CREATE_SQL_PATCH
- A SQL patch, as used by this procedure, is a set of user specified hints for specific statements identified by the SQL text
- When considering this as a vulnerability consider the following
 - By default EXECUTE is granted to PUBLIC
 - Hints can be used to override configuration settings such as PARALLEL DEGREE and have the effect of substantially degrading performance and oversubscribing resources

```
dbms_sqldiag.create_sql_patch(  
  sql_text  IN CLOB,  
  hint_text IN CLOB,  
  name      IN VARCHAR2 := NULL,  
  decription IN VARCHAR2 := NULL,  
  category  IN VARCHAR2 := NULL,  
  validate  IN BOOLEAN  := TRUE)  
RETURN VARCHAR2;
```

```
SQL> DECLARE  
  2   stxt CLOB := 'SELECT /* CREATE_PATCH2 */ COUNT(*), MAX(siid)  
FROM uwclass.serv_inst WHERE srvr_id = :srvrid';  
  3   htxt CLOB := 'BIND_AWARE';  
  4   retVal VARCHAR2(60);  
  5 BEGIN  
  6   retVal := sys.dbms_sqldiag.create_sql_patch(stxt, htxt);  
  7 END;  
  8 /
```

PL/SQL procedure successfully completed.

An IT Terrorist Attack (7:7)

- How many of Oracle's vulnerability enhancing defaults such as grants of EXECUTE to PUBLIC have you disabled?
- No better time to start than tomorrow

