Issues with the initialisation parameter "fixed_date"

By Pete Finnigan

This very short paper descibes the initialisation parameter "fixed_date" and the short comings of not protecting access to this parameter and also the issues that can arise with the use of `SYSDATE` and this parameter.

The problem

Quite a number of applications take advantage of the built in date features of Oracle and ease with which the current date time can be selected and used within functionality. I have seen a few financial applications where interest payments and schedules are based and calculated with help from the date returned from `SYSDATE`. Imagine the calculation errors that could occur if the system date was incorrect when interest payments were calculated or overdue payments were not collected on time because the system used an incorrect date.

The initialisation parameter *fixed_date* can be set in the initialisation file init{SID}.ora or can be added or changed using the command `ALTER SYSTEM`. This parameter lets you set a constant date that `SYSDATE` will always return instead of the current date. The date format is `YYYY-MM-DD-HH24:MI:SS`. You can also specify the Oracle date format without the time element in the initialisation file i.e.

```
fixed_date="30-nov-2001"

or

fixed_date = 30-nov-2001
```

Specify with double quotes or none at all but not single quotes. Oracle state that this parameter is primarily used for testing

The bad news

The bad news is that an attacker or malicious user if they knew that critical functionality or calculations are dependent on the `SYSDATE` could use this parameter to their advantage. All that is needed is to find a user who has the privilege `ALTER SYSTEM` or a user that has the rights to grant this privilege and then the attacker could change the date at the time they access your application or before overnight batch runs start and cause havock.

An Example

Here is an example of a few commands to demonstrate the above problem.

```
SQL> sho user
USER is "SYS"
SQL> select grantee
```

```
  2  from dba_sys_privs
  3  where privilege='ALTER SYSTEM';

GRANTEE
------------------------------
CTXSYS
DBA
MDSYS
PORTAL30
PORTAL30_SSO

SQL> connect portal30/portal30
Connected.
SQL> select sysdate
  2  from dual;

SYSDATE
---------
19-NOV-01

SQL> alter system set fixed_date='2001-11-01';

System altered.

SQL> select sysdate
  2  from dual;

SYSDATE
---------
01-NOV-01

SQL> connect dbsnmp/dbsnmp
Connected.
SQL> select to_char(sysdate,'DD-MON-YYYY')
  2  from dual;

TO_CHAR(SYS
-----------
01-NOV-2001

SQL> connect sys/change_on_install
Connected.
SQL> select grantee
  2  from dba_sys_privs
  3  where privilege='ALTER SESSION';

GRANTEE
------------------------------
CONNECT
CTXSYS
DBA
MDSYS
PORTAL30
PORTAL30_SSO
RECOVERY_CATALOG_OWNER

7 rows selected.

SQL> connect ctxsys/ctxsys
Connected.
SQL> alter session set fixed_date='2001-10-12';
```

```
alter session set fixed_date='2001-10-12'
                  *
ERROR at line 1:
ORA-02096: specified initialization parameter is not modifiable with
this
option


SQL>
```

The above example shows first that we connect as a user who is able to select privileges from the *dba* view *dba_sys_privs* and we check which users have the permission `ALTER SYSTEM`. There are as we can see a number of default users and the `DBA` role. we could check further at this stage to see which users have this role, but we won't in this example. We then connect as one of the users *portal30* using its default password. Next we then check `SYSDATE` is showing the correct date and then alter the parameter *fixed_date* and re-check that `SYSDATE` has indeed changed. Finally we can then log in as another user and confirm that the `SYSDATE` is incorrect for all users.

The last part of the script just shows that you cannot change the *fixed_date* parameter with only the `ALTER SESSION` privilege.

Conclusions

Clearly this parameter could be very dangerous if an application uses `SYSDATE` in its functionality. If the date is critical you should consider not using `SYSDATE`, which in some cases is not easy. At least review which users have the privilege `ALTER SYSTEM` and restrict access to this privilege. Also ensure that the default users that are not needed are removed or the passwords changed. Also any default users that are needed have the default passwords changed. For a paper on default passwords see default-user.htm.

About Pentest

Established in 2001, Pentest Limited is a leading international provider of IT security, specialising in Web Application Security and Penetration Testing services. Pentest provides independent, practical advice to a wide range of clients across the UK, Europe, USA and Asia. For more information, or for further details about Pentest's services, please visit www.pentest.co.uk or call +44 (0) 161 233 0100.