

Cursor Snarfing

Cursor Snarfing in Oracle

In Oracle RDBMS 11gR2, Oracle introduced some countermeasures on "Cursor Snarfing" in DBMS_SQL.

Background: Users had been able to obtain access to other peoples cursors which had not been closed properly.

These security changes in Oracle 11 can cause problems with code developed for and running in Oracle 10 (ORA-29471). If code refactoring is not possible, for example by changing syntax to NDS ("execute immediate"), one of these workarounds may be helpful:

- change dbms_sql.open_cursor syntax to:

```
curs = dbms_sql.open_cursor(level);
```

Where level = 0. Unfortunately, there is an open Oracle bug at least affecting Solaris where this results in ORA-29744.

- disable countmeasures globally by setting

```
alter system set "_dbms_sql_security_level" = 384 scope=spfile;
```

See also:

- [David Litchfield's Weblog](#)
- [MOS Note: 1298367.1](#)
- [MOS Note: 556301.1](#)
- [Oracle® Database PL/SQL Packages and Types Reference 11g Release 2](#)