CVE-2010-2411: Oracle SYS.DBMS_IJOB – Job manipulation vulnerability

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. Once a job is submitted, it is assigned a job number that can be used later for job administration. DBMS_IJOB is a package used internally by DBMS_JOB to implement some of its functionality. This package contains job manipulation procedure that do not check for job ownership.

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 a data integrity vulnerability in the DBMS_IJOB package.

Findings

An attacker can use the procedure within the DBMS_IJOB to manipulate jobs submitted by other users. Thus an attacker can effectively stop the execution of critical jobs.

Details

When calling administration procedures in DMBS_IJOB with a job number that does not exists, an error is raised with an appropriate message. If the job does exist, regardless of its owner, the procedure is executed successfully and job is altered. The following DBMS_IJOB procedures can be executed:

- REMOVE
- NEXT_DATE
- INTERVAL
- BROKEN
- CHANGE_ENV
- DROP_USER_JOBS

Exploit

By calling to the procedures with valid job numbers, their definition is altered.

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