CVE-2010-2411: Oracle SYS.DBMS_IJOB – Privilege Elevation 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. The procedure WHAT is used to alter the task code of existing job. DBMS_IJOB is a package used internally by DBMS_JOB to implement some of its functionality. This package contains a WHAT 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 a privilege elevation vulnerability in the DBMS_IJOB package.

Findings

An attacker can use the DBMS_IJOB.WHAT procedure to change the PL/SQL code executed by a job that is owned by a higher privileged user. Thus an attacker can effectively execute arbitrary PL/SQL code with the security content of any database user who owns an active job.

Details

When calling DMBS_IJOB.WHAT 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 the PL/SQL code to be executed by the job is replaced with the value of the "what" parameter for the call. This code will be executed with security privileges of the original job owner.

Exploit

Assume 41 is the number of a job that belongs to an administrative user. Then the following code can be used to grant a user with DBA privileges:

```
begin
  sys.dbms_ijob.what(41, 'EXECUTE IMMEDIATE (''GRANT DBA TO SCOTT'');');
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