



**Understanding Your Risk to the Zero-Day Privilege Escalation Oracle
JAVA Packages Vulnerability Using DbProtect**

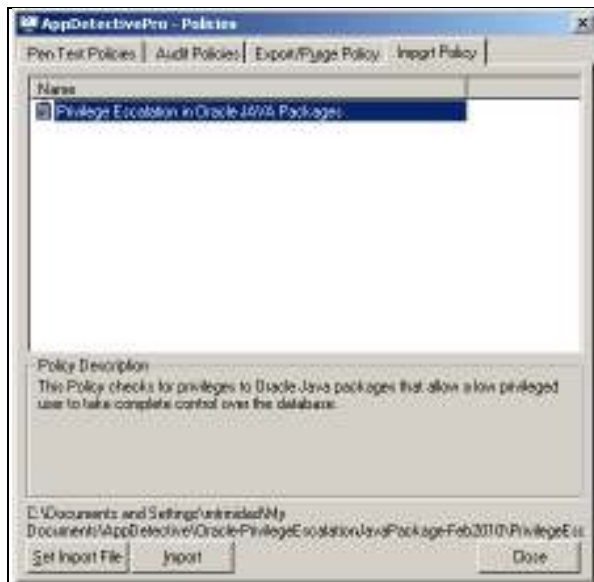
- 1) Download the Privilege Escalation in Oracle JAVA Packages audit policy from the following link and save it to a file directory:
 - http://www.appsecinc.com/resources/alerts/oracle/2010-DBMS_JVM_EXP_PERMS.shtml
- 2) Unzip the PrivilegeEscalationOracleJava.zip file.
- 3) Open the Policy Editor to import the policy. Click on the Import Policy tab and click on the Set Import File button. Browse to the file directory where you saved the PrivilegeEscalationOracleJava.abd file. Select this file and click Open. Select the Privilege Escalation in Oracle JAVA Packages and click on Import. This will import the file and make it available for use when running an Audit.



AppDetectivePro Policy Editor

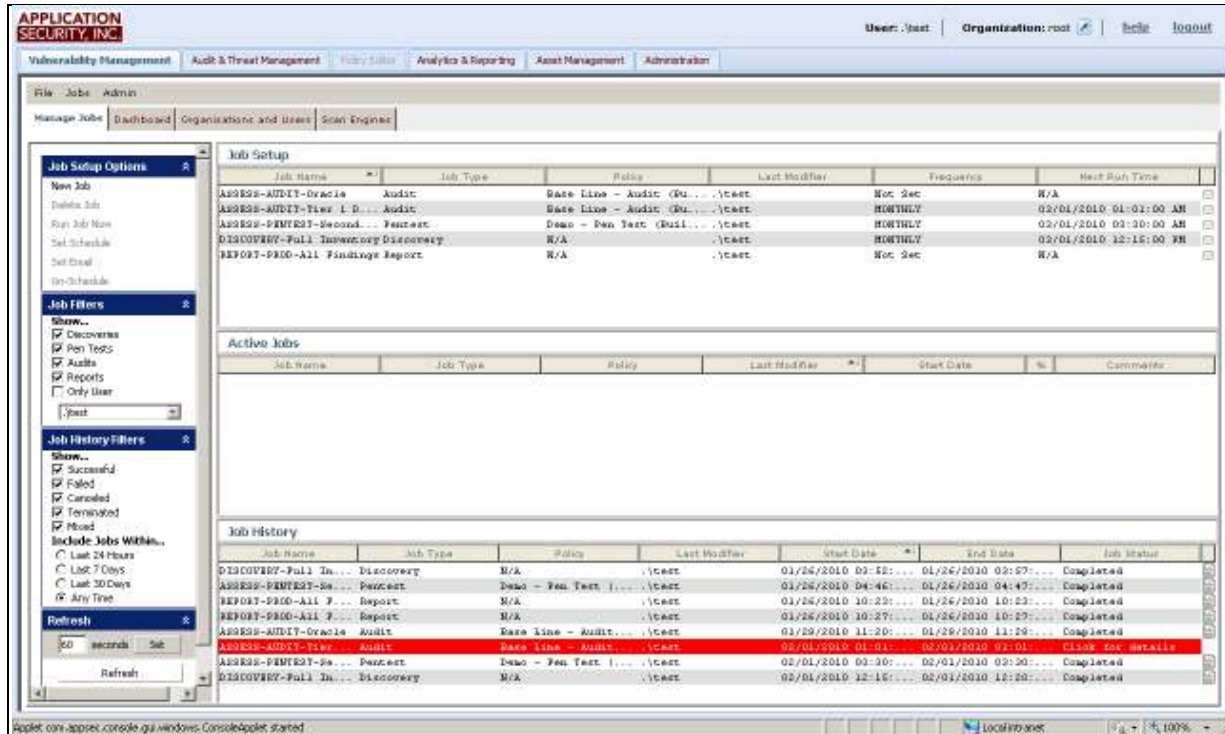


Browse and Import the .abd file



Select the Policy and Import

- 4) Log into DbProtect and click on the Vulnerability Management tab. Click on the Manage Jobs tab. You can choose to do several things:
 - Run a new Discovery job to look for Oracle databases to validate you have an understanding your entire Oracle environment.
 - Run a new Audit job and add all Oracle databases into the new job. Select the Privilege Escalation in Oracle JAVA Packages policy to use for the audit.
 - Edit an existing Audit job that is used on all your Oracle databases and use the new Privilege Escalation in Oracle JAVA Packages policy.
 - Be sure to 'Enable Auto Report' for the Vulnerability Details quickly review the results of the Audit.



Run an Audit job with the new Privilege Escalation in Oracle JAVA Packages policy to Understand your Risk

- Review the results of the Vulnerability Details report. The Audit results from the policy will identify for each Oracle databases scanned if it is vulnerable. The policy will identify if the EXECUTE privilege on each of the vulnerable JAVA packages is granted to PUBLIC.

Test Date: 2/8/2010 11:42:58 AM - 2/8/2010 11:43:00 AM
Vulnerability Details

Application: Oracle11g Database (ORCL) on 172.16.20.17 (test11g.slab.prv), port 1621

✘ High Risk
 ⚠ Medium Risk
 ? Low Risk
 i Informational

✘ EXECUTE on DBMS_JAVA Packages GRANTED to PUBLIC Continued from previous page...

Overview: A Privilege Escalation vulnerability has been announced by a security researcher that allows an attacker to take complete control of an Oracle database system. Three packages related to 'Aurora' - Oracle's JAVA system are vulnerable, all of which are by default accessible to any user in the database. There is currently no patch available to correct this issue, however Oracle offers access control features that can easily be configured to eliminate or reduce the risk posed by this vulnerability.

This attack requires EXECUTE privileges on the following packages:

- SYS.DBMS_JAVA
- SYS.DBMS_JAVA_TEST
- SYS.DBMS_JVM_EXP_PERMS

By default, PUBLIC is granted EXECUTE on all three.

Fix/Recommendations: There is currently no patch available for this vulnerability. However, Oracle offers access control features that can be configured to eliminate or reduce the risk posed by this issue.

Revoking EXECUTE privileges on the vulnerable packages is the most effective means to protect your systems. First, revoke execute privileges from PUBLIC, then perform a User Rights Review scan to determine if any users can still EXECUTE the vulnerable packages. Revoke any privileges on these packages that are not strictly required to perform job functions.

For those circumstances where database users or roles must be granted EXECUTE rights on the vulnerable DBMS_JAVA packages, we recommend monitoring the use of those packages using DbProtect's Audit & Threat Management module to ensure no exploits are attempted.

The following scripts can be used to REVOKE privileges on the vulnerable packages from PUBLIC. However, before executing these scripts on a production system be sure to test the changes to ensure they do not cause functional issues with applications using the database.

```

REVOKE EXECUTE on SYS.DBMS_JAVA from PUBLIC;
REVOKE EXECUTE on SYS.DBMS_JAVA_TEST from PUBLIC;
REVOKE EXECUTE on SYS.DBMS_JVM_EXP_PERMS from PUBLIC;

```

Vulnerability Details:

(col1=PUBLIC) (col2=DBMS_JAVA_TEST) (col3=EXECUTE)
(col1=PUBLIC) (col2=DBMS_JVM_EXP_PERMS) (col3=EXECUTE)
(col1=PUBLIC) (col2=DBMS_JAVA) (col3=EXECUTE)

Number of Vulnerabilities Found For Check:

Review the Audit Results for each Oracle database scanned

- To understand which users and roles have EXECUTE privilege on each of the Oracle JAVA packages, you can run a User Rights Review scan on each of the Oracle databases identified as vulnerable using AppDetectivePro. Contact your Account Manager for more details.