
PeteFinnigan.com security advisory – DBMS_SCHEDULER

Description

The new scheduler functionality added for Oracle 10gR1 allows jobs to be configured to run on the host operating system. This functionality can be abused by any authenticated user with the CREATE JOB system privilege. It is possible to gain DBA rights, gain remote OS access, create a remote reverse shell or start an xterm remotely.

Risk

Any user with CREATE JOB and access to the DBMS_SCHEDULER package can exploit these bugs.

Workaround

It is not possible to work around this issue if the DBMS_SCHEDULER package is used. If not then access can be revoked from the package from PUBLIC along with revoking the CREATE JOB system privilege.

Patch information

We advise customers of Oracle to apply the patches listed in the alert #68 as soon as possible. Please see Metalink document ID 281189.1 at

http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=281189.1

References

Oracles advisory can be found here -

<http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf>

This alert also references many other fixes found by many other researchers. Their advisories can be found here:

- <http://www.appsecinc.com/resources/alerts/oracle/>
- <http://www.integrigy.com/resources.htm>
- <http://www.nextgenss.com/advisory.htm>
- <http://www.red-database-security.com>
- http://www.qinetiq.com/home/case_studies/security.html
- <http://www.securityfocus.com/bid/10871>
- <http://www.kb.cert.org/vuls/id/316206>

Credit

These issues were found by Pete Finnigan of PeteFinnigan.com in conjunction with Jonathan Gennick of O'Reilly and Alexander Kornbrust of Red Database security.