
PeteFinnigan.com security advisory – DIRECTORY OBJECT – Reading outside of the directory object

Description

Directory objects used in the Oracle database contain the location of a specific operating system directory. This location can then be used from database packages and functions by accessing the DIRECTORY objects in various ways. It is possible to abuse directory object.

Risk

Any existing DIRECTORY object that can be accessed presents a potential risk. Read privileges on a DIRECTORY object are required to exploit this issue.

Workaround

If no directory objects exist that can be accessed then the problem can be minimised. Review existing directory objects and their access privileges in the database. A good script is http://www.petefinnigan.com/who_can_access.sql which can be used to ascertain which users can access directory objects. Revoke read access privileges from these objects and also ensure no users have DIRECTORY object creation or alteration system privileges.

Patch information

We advise customers of Oracle to apply the patches listed in the CPU – January 2005 advisory as soon as possible. Please see Metalink document ID 293737.1 at

http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=293737.1

Patches are available for other components affected by other bugs in this Oracle advisory. See the Oracle advisory for details.

References

Oracles advisory can be found here - http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-2005_advisory.pdf

Credit

This issue was found by Pete Finnigan of PeteFinnigan.com.