FAQ – Script for Fix for Oracle Security Alert CVE-2012-1675

CONFIDENTIAL INFORMATION

DISCLAIMER

TRADEMARKS

Document released: June 2012

Web address: http://www.exlibrisgroup.com

Question: What is this Security Patch About?

This security alert addresses the security issue CVE-2012-1675 – vulnerability in the TNS listener (referred to as the "TNS Listener Poison Attack") that affects the Oracle database server. This vulnerability may be remotely exploitable without authentication, that is, it may be exploited over a network without the need for a username and password. A remote user can exploit this vulnerability to affect the confidentiality, integrity, and availability of systems that do not have the recommended solutions applied. In order to prevent such an attack, reconfigure the listener using COST (Class of Secure Transport) to restrict instance registration with database listeners. With the COST restriction in place, only local instances are able to register.

About COST

The COST parameters specify a list of transports that are considered secure for the administration and registration of a particular listener. The COST parameters identify which transports are considered secure for that installation and whether the administration of a listener requires secure transports. COST does not affect client connections utilizing other protocols.

To protect the listener using COST, restrict registration to the IPC protocol .If the listener is configured to accept registration requests that use the IPC protocol, only databases running on the same machine with the listener are able to register.

Note: The vulnerability described in this document comes only from databases created on the same network (on another server).

Question: What Does the Script Supplied by ExLibris Do?

The script changes the `listener.ora` files under any `$ORACLE_HOME/network/admin` directory on the DB server. It also changes the DB parameter `local_listener` to use the IPC protocol for all DBs on the server.

For a detailed description of the script and instructions on how to use it, refer to the document *Oracle Security Alert CVE-2012-1675 – Implementation Clarifications for Automatic Fix*.

Question: What Happens If the Fix is Not Applied?

The application and DB will continue as usual. The only risk is the one described above.

Question: Can I Rollback the Changes?

Yes. ExLibris supplies a rollback script.