



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

CONFIDENTIAL INFORMATION

The information herein is the property of Ex Libris Ltd. or its affiliates and any misuse or abuse will result in economic loss. DO NOT COPY UNLESS YOU HAVE BEEN GIVEN SPECIFIC WRITTEN AUTHORIZATION FROM EX LIBRIS LTD.

This document is provided for limited and restricted purposes in accordance with a binding contract with Ex Libris Ltd. or an affiliate. The information herein includes trade secrets and is confidential.

DISCLAIMER

The information in this document will be subject to periodic change and updating. Please confirm that you have the most current documentation. There are no warranties of any kind, express or implied, provided in this documentation, other than those expressly agreed upon in the applicable Ex Libris contract. This information is provided AS IS. Unless otherwise agreed, Ex Libris shall not be liable for any damages for use of this document, including, without limitation, consequential, punitive, indirect or direct damages.

Any references in this document to third-party material (including third-party Web sites) are provided for convenience only and do not in any manner serve as an endorsement of that third-party material or those Web sites. The third-party materials are not part of the materials for this Ex Libris product and Ex Libris has no liability for such materials.

TRADEMARKS

"Ex Libris," the Ex Libris bridge, Primo, Aleph, Alephino, Voyager, SFX, MetaLib, Verde, DigiTool, Preservation, URM, Voyager, ENCompass, Endeavor eZConnect, WebVoyage, Citation Server, LinkFinder and LinkFinder Plus, and other marks are trademarks or registered trademarks of Ex Libris Ltd. or its affiliates.

The absence of a name or logo in this list does not constitute a waiver of any and all intellectual property rights that Ex Libris Ltd. or its affiliates have established in any of its products, features, or service names or logos.

Trademarks of various third-party products, which may include the following, are referenced in this documentation. Ex Libris does not claim any rights in these trademarks. Use of these marks does not imply endorsement by Ex Libris of these third-party products, or endorsement by these third parties of Ex Libris products.

Oracle is a registered trademark of Oracle Corporation.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Ltd.

Microsoft, the Microsoft logo, MS, MS-DOS, Microsoft PowerPoint, Visual Basic, Visual C++, Win32,

Microsoft Windows, the Windows logo, Microsoft Notepad, Microsoft Windows Explorer, Microsoft Internet Explorer, and Windows NT are registered trademarks and ActiveX is a trademark of the Microsoft Corporation in the United States and/or other countries.

Unicode and the Unicode logo are registered trademarks of Unicode, Inc.

Google is a registered trademark of Google, Inc.

Copyright Ex Libris Limited, 2012. All rights reserved.

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.