



Oracle Security Alert CVE-2012-1675 – Implementation Clarifications for Automatic Fix

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: July 1, 2012

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

Table of Contents

1	Purpose	4
2	General Description	4
3	Oracle Versions Affected	4
4	General Recommendations	4
5	Assumptions	4
	<i>More Than one SID is Active for the Latest Software Version</i>	5
	<i>Noexec Mount Option on /tmp</i>	6
6	Detailed Description and Execution Instructions	6
7	Success Validation	8
8	Script Output	9
9	Troubleshooting	11
	<i>Bad tnsnames.ora File</i>	11
	<i>More Than one SID is Active for the Latest Software Version</i>	12
	<i>Noexec Mount Option on /tmp</i>	13
10	Appendix A - Running the fix_init.bash Script	13
11	Appendix B – Checking if the DB is Updated	13
12	Appendix C – Rolling Back the Listener Configuration Change	14

Purpose

This document describes the script supplied by Ex Libris in order for you to apply the solution suggested by the Oracle corporation for Oracle Security Alert CVE-2012-1675 (May 2012).

General Description

The script applies a fix to the Oracle Listener component. It aims to fix a potential security problem from external attack that utilizes the `EXTPROC` service. The fix replaces `EXTPROC` in the listener configuration file with `REGISTER` and sets the `local_listener` DB parameter to `REGISTER`, using the IPC protocol.

Note :

Implementation requires a short downtime for an application restart. In some cases, it may require also a DB restart (see [Assumptions](#) on page 4).

Oracle Versions Affected

The Oracle 10g and 11g databases are affected.

General Recommendations

- Back up both the Oracle SW and DB before running any update.
- Run the routine on the test server before production.

Assumptions

- The script is valid only for a single DB configuration. **Do not** apply this fix for an RAC configuration.
- The script is being run as the `root` user.

- The script is being run for the latest version of Oracle software that exists on the server, so that if the server includes both `/exlibris/app/oracle/product/102` and `/exlibris/app/oracle/product/11r2`, the script starts the listener from the `/exlibris/app/oracle/product/11r2` environment.

For Voyager Customers, the script starts the listener from

`/oracle/app/oracle/product/10.2.0/db_1` or
`/oracle/app/oracle/product/11.2.0/db_1`

- The script uses the `oratab` file to identify the SIDs and `ORACLE_HOMES` that exists on the server. The `oratab` file is under the `/etc` directory for Linux and AIX and under the `/var/opt/oracle` directory for Solaris. **If an SID is marked in the `oratab` file with an N, the script does not recognize it.**
- The script takes from the `oratab` file only those SIDs whose software is installed under `/exlibris/app/oracle/product` or `/oracle/app/oracle/product` (Exlibris standard installations).
- The script runs from the latest version of Oracle on the server. The listener is started from that version only.
- If the latest version of Oracle includes more than one SID, the script runs only for the active SID. If both SIDs are active, the script quits and does not perform the update. In this case, contact Ex Libris support, or use the workaround described in the [Troubleshooting](#) section
- The script updates the older listener files and DBs on the server, if there are any.
- If `spfile` does not exist for an older DB on the server, the DB needs to be restarted for the change to take effect. A message that the DB is down is displayed. Connecting to this DB is not possible until the DB is restarted.
- If `spfile` does not exist for the DB to be updated (the latest version of Oracle), the script quits and displays a message. Run the `fix_init.bash` script supplied under the same directory to create the `spfile` (see [If the `tnsnames.ora` file has been changed](#) and the application is running on another server, copy the new `tnsnames.ora` file to that application server under `$ORACLE_HOME/network/admin`

More Than one SID is Active for the Latest Software Version

If more than one SID is active for the latest software version, the following error is displayed:

```
-----
Found 2 SIDs for /exlibris/app/oracle/product/11
-----
Exiting...
```

As a workaround, mark one of the active SID's in the `oratab` file described above as N, and run the script again.

For example:

```
arc4:/exlibris/app/oracle/product/11r2:N
```

When the script finishes, issue the following command as the `oracle` user for the DB that is marked `N`. For example:

```
setenv ORACLE_SID arc4
sqlplus '/as sysdba'
alter system set
local_listener='(DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=REGISTER)))'
scope=both;
create pfile from spfile;
```

Noexec Mount Option on /tmp

If the following error is displayed:

```
# ./ora_listener_patch
Verifying archive integrity... All good.
Uncompressing Fix For Oracle Listener Security Issue.....
./ora_listener_patch: ./ora_listener_patch.bash: /bin/bash: bad
interpreter: Permission denied
```

The `/tmp` directory may be configured with noexec mount options. Use the following syntax to run the script:

```
TMPDIR=/exlibris/ftp_from_exlibris/ ./ora_listener_patch
```

- Appendix A - Running the `fix_init.bash` Script on page [12](#)).

Note: Running the `fix_init.bash` script restarts the DB. Then execute the main script again.

Detailed Description and Execution Instructions

The script changes the `listener.ora` file for all Oracle software running on the server and restarts the listener. For more information, refer to the document *FAQ – Script for Fix for Oracle Security Alert CVE-2012-1675*.

The script also changes the DB parameter `local_listener` for all DBs that exist on the server according to the `/etc/oratab` file.

The script accepts two parameters:

- The Ex Libris customer code
- The products for which you want to run the script (that exist on the specified DB server)

For example:

```
Please enter Ex Libris customer code (country code + customer):
01UDQ
Please enter the products that you would like to patch (product1, product2
...):
Aleph,Primo
```

If you need to check if the new configuration was already done for the DB, use the procedure described in [Appendix B – Checking if the DB is Updated](#) on page 13.

To execute the script, perform the following commands. (Execute the following as the root or sudo user):

```
su - root //or use 'sudo' with relevant permissions

cd /exlibris/ftp_from_exlibris

/exlibris/product/bin/wget --passive-ftp
ftp://orasec:kl,,euus@ftp.exlibris-usa.com/ora_listener_patch

chmod +x ora_listener_patch

./ora_listener_patch
```

Note: If you receive an error from wget, use the `which wget` command to locate the correct path and use it in the command above.

- For Voyager Customers running on Unix:

```
su - root //or use 'sudo' with relevant permissions

cd /ml/incoming
ftp ftp.exlibris-usa.com
user: orasec
password: kl,,euus
bin
get ora_listener_patch
bye

chmod u+x ./ora_listener_patch
./ora_listener_patch

// Customers on Voyager 7.2.x and earlier must have voyager restarted.
// It is optional for Voyager 8.0.0 and higher
/etc/init.d/voyager stop
/etc/init.d/voyager start
```

- For Voyager Customers running on Windows:

```
cd d:/incoming
ftp ftp.exlibris-usa.com
user: patch
password: s70ra&e
cd oracle/scripts
```

```
bin
get ora_listener_patch.exe
bye

./ora_listener_patch.exe

./ora_listener_patch.exe

// Customers on Voyager 7.2.x and earlier must have voyager restarted.
// It is optional for Voyager 8.0.0 and higher
c:
cd c:/etc/init.d/
VOYAGER.KSH STOP
VOYAGER.KSH START
```

Note:

Window's users enter commands using the kornshell application. To open a kornshell environment, go to **Start>All Programs>MKS Toolkit>Kornshell** or click the Kornshell icon on your desktop.

The script output is spooled to the /tmp/listener_config_output.{date in the format: YYYY-MM-DD.HHMMSS}.log file.

Success Validation

To check the script success, log on as the application user on the application (UNIX) servers, and check that the sqlplus connection is still valid using the environment variable <application>_db.

Use:

```
<schema_name>/<schema_name>@<application>_db
```

For example:

- As aleph:

```
su - aleph
sqlplus aleph/aleph@$aleph_db
```

- As primo:

```
su - primo
sqlplus primo/primo@$primo_db
```

- As voyager:

```
su - voyager
sqlplus <username>/<password>@VGER
```


If the connection fails, review and follow the instructions in the [Troubleshooting](#) section on page 11.

If problem still occurs, contact Ex Libris support.

Note:

Choose a valid schema name/password to perform the validation.

Script Output

Assuming, for example, ORACLE_SID is prm4, and prm2 from an older version is also running on the server, the output looks like the following:

```
== Applying oracle patch fix for Listener on
/exlibris/app/oracle/product/11r2 for prm4
= related to Oracle Security Alert for CVE-2012-1675, issued 2012 April
-----
Updating the local_listener parameter
-----
-----
spfile exists - setting local_listener parameter
-----

SQL*Plus: Release 11.2.0.3.0 Production on Sun May 20 09:53:08 2012

Copyright (c) 1982, 2011, Oracle. All rights reserved.

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit
Production
With the Partitioning, OLAP, Data Mining and Real Application Testing
options

sys@PRM4> sys@PRM4>
System altered.

sys@PRM4>
File created.

sys@PRM4> Disconnected from Oracle Database 11g Enterprise Edition Release
11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing
options
-----
Stopping Oracle Listener
-----

LSNRCTL for Solaris: Version 11.2.0.3.0 - Production on 20-MAY-2012
09:53:12

Copyright (c) 1991, 2011, Oracle. All rights reserved.
```

```

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP) (HOST=il-
sundba01) (PORT=1521)))
The command completed successfully
WORKDIR is /exlibris/ftp_from_exlibris/listener_sec_config
-----
Appending SECURE_REGISTER_LISTENER = (IPC) line to listener.ora
-----
Displaying /exlibris/app/oracle/product/11r2/network/admin/listener.ora
-----

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP) (HOST = il-sundba01) (PORT = 1521))
      (ADDRESS = (PROTOCOL = IPC) (KEY = REGISTER))
    )
  )
sid_list_listener=(sid_list=
                    (sid_desc=
                      (global_dbname=prm43.il-
sundba01.corp.exlibrisgroup.com.)
                      (sid_name=prm43)

(oracle_home=/exlibris/app/oracle/product/11r2)
                    )
                    (sid_desc=
                      (global_dbname=prm4.il-
sundba01.corp.exlibrisgroup.com..)
                      (sid_name=prm4)

(oracle_home=/exlibris/app/oracle/product/11r2)
                    )
                    )
SECURE_REGISTER_LISTENER = (IPC)
-----
Restarting the listener
-----
Updating prm2 with listener condiguration
-----
spfile exists for prm2
DB prm2 is up and running

System altered.

-----
== Oracle Listener security patch is complete for instance prm4 on il-
sundba01
-----
== Please review
-----
== Sun May 20 09:53:55 IDT 2012

```

If the script finds that the DB parameter has already been set, the following message is displayed:

```
-----  
The parameter local_listener already set to KEY=REGISTER - OK  
-----
```

If the script finds the appropriate REGISTER line in the listener.ora file, the following message is displayed:

```
-----  
SECURE_REGISTER_LISTENER = (IPC) line already present - OK  
-----
```

Troubleshooting

Bad tnsnames.ora File

If an ORA error message is displayed when trying to connect from the application server using sqlplus, verify that the service_name section in the \$ORACLE_HOME/network/admin/tnsnames.ora file and the global_dbname section in the \$ORACLE_HOME/network/admin/listener.ora file are **identical**.

If, for example, the tnsnames.ora file looks like the following (see the highlighted text in red):

```
il-primoqa01.prm4=(description=  
    (address=  
        (protocol=ipc)  
        (key=prm4))  
    (address=  
        (protocol=tcp)  
        (host=il-primoqa01)  
        (port=1521))  
    (connect_data=(service_name=prm4) (server=DEDICATED)))
```

And the listener.ora file looks like the following:

```
LISTENER =  
  (DESCRIPTION_LIST =  
    (DESCRIPTION =  
      (ADDRESS = (PROTOCOL = TCP) (HOST = il-  
primoqa01.corp.exlibrisgroup.com) (PORT = 1521))  
      (ADDRESS = (PROTOCOL = IPC) (KEY = REGISTER))  
    )  
  )  
  sid_list_listener=(sid_list=  
  
    (sid_desc=  
      (global_dbname=prm4.il-  
primoqa01.corp.exlibrisgroup.com)  
      (sid_name=prm4)
```

```
(oracle_home=/exlibris/app/oracle/product/11r2)
    )
    (sid_desc=
        (global_dbname=prm3.il-
primoqa01.corp.exlibrisgroup.com)
        (sid_name=prm3)

    (oracle_home=/exlibris/app/oracle/product/112)
    )
    )
startup_wait_time_listener=0
connect_timeout_listener=20
trace_level_listener=off
SECURE_REGISTER_LISTENER = (IPC)
```

Append the full service_name in the tnsnames.ora file. For example:

```
il-primoqa01.prm4=(description=
    (address=
        (protocol=ipc)
        (key=prm4))
    (address=
        (protocol=tcp)
        (host=il-primoqa01)
        (port=1521))
    (connect_data=(service_name= prm4.il-
primoqa01.corp.exlibrisgroup.com) (server=DEDICATED)))
```

Note: If the tnsnames.ora file has been changed and the application is running on another server, copy the new tnsnames.ora file to that application server under \$ORACLE_HOME/network/admin

More Than one SID is Active for the Latest Software Version

If more than one SID is active for the latest software version, the following error is displayed:

```
-----
Found 2 SIDs for /exlibris/app/oracle/product/11
-----
Exiting...
```

As a workaround, mark one of the active SID's in the oratab file described above as N, and run the script again.

For example:

```
arc4:/exlibris/app/oracle/product/11r2:N
```

When the script finishes, issue the following command as the oracle user for the DB that is marked N. For example:

```
setenv ORACLE_SID arc4
sqlplus '/as sysdba'
```

```
alter system set
local_listener='(DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=REGISTER)))'
scope=both;
create pfile from spfile;
```

Noexec Mount Option on /tmp

If the following error is displayed:

```
# ./ora_listener_patch
Verifying archive integrity... All good.
Uncompressing Fix For Oracle Listener Security Issue.....
./ora_listener_patch: ./ora_listener_patch.bash: /bin/bash: bad
interpreter: Permission denied
```

The /tmp directory may be configured with noexec mount options. Use the following syntax to run the script:

```
TMPDIR=/exlibris/ftp_from_exlibris/ ./ora_listener_patch
```

Appendix A - Running the fix_init.bash Script

The script accepts ORACLE_SID as a parameter.

As the `oracle` user of the latest version of the Oracle software on the server, execute the following:

```
cd /exlibris/ftp_from_exlibris/ORACLE_LISTENER_PATCH
bash fix_init.bash <ORACLE_SID>
```

For example:

```
bash fix_init.bash prm4
```

Appendix B – Checking if the DB is Updated

In order to check if the DB is already configured with the new listener configuration, execute the following procedure as the UNIX `oracle` user:

```
su - oracle
cd /exlibris/ftp_from_exlibris/ORACLE_LISTENER_PATCH

chmod u+x ./verify_listener_config.bash

./verify_listener_config.bash
```

Appendix C – Rolling Back the Listener Configuration Change

In order to roll back the listener configuration fix, execute the following procedure as the UNIX `oracle` user:

```
su - oracle
cd /exlibris/ftp_from_exlibris/ORACLE_LISTENER_PATCH
bash rollback_listener_config.bash
```