Database Security Brief: The Oracle Critical Patch Update for April 2007

David Litchfield (davidl@ngssoftware.com)

18th April 2007

On the 17th April 2007 Oracle released their 10th Critical Patch Update. This brief discusses the database flaws and EM01 which relates to the Intelligent Agent. Many of the flaws being patched are old issues. For example, DB01 relates to an issue first reported to Oracle in 2002 and another in June 2004. This may indicate that Oracle are now in a position where they can "clear the backlog" indicating that most of the more important flaws have been found and patched. If this is correct then we should see smaller patches being released in future CPUs. That said, between myself, Paul Wright and Mark Litchfield, NGSSoftware has reported a further 39 issues that are still awaiting a patch many of which we would rate as high risk. NGSSQuirreL for Oracle can positively identify these flaws in a database server. Anyway, enough of the predictions about future CPUs and onto this one:

DB01 Authentication Bypass on Oracle running on Windows XP

Due to the way that Windows XP with Simple File Sharing enabled logs on users it is possible for an attacker to gain DBA access to the Oracle server. I initially reported this flaw to Oracle in 2002.
Ref: http://www.ngssoftware.com/papers/database-on-xp.pdf

DB02 Race Condition in the RLMGR_TRUNCATE_MAINT trigger

In 10g Release 2 there is a trigger called RLMGR_TRUNCATE_MAINT owned by EXFSYS. It executes when a user issues a TRUNCATE statement on a table. Part of the trigger executes the following:

```
begin
 select rset_pack into rcpcknm from rlm$ruleset where
 rset_owner = objown and rset_name = objnm
 and bitand(rset_prop, 4) = 4;
 if (sys.exf$dbms_expfil_syspack.proc_is_definers(
objown, rcpcknm, 'TRUNCATE_RCTAB') = 0) then
  dbms_rlmgr_dr.raise_error(41682);
           end if;
  EXECUTE IMMEDIATE
'begin "'||objown||'".'||rcpcknm||'.TRUNCATE_RCTAB; end;';
exception
  when no_data_found then null;
end;
```

This code calls the exf$dbms_expfil_syspack.proc_is_definers function. This function checks whether the named package is set to DEFINER or CURRENT_USER for the AUTHID column of DBA_PROCEDURES. If it's DEFINER, then the function returns a non-zero value. This is then checked in the trigger and if the return value is non-zero the TRUNCATE_RCTAB procedure of the package is executed. If during the time of the SELECT performed by exf$dbms_expfil_syspack.proc_is_definers and the EXECUTE IMMEDIATE the package can be re-specified as CURRENT_USER then it's possible to run code as the EXFSYS user and gain its privileges. As you can guess that doesn't leave much time and, like most race conditions, is notoriously difficult to exploit. PL/SQL race conditions and this particular flaw are discussed in the Oracle Hacker's Handbook. This was reported to Oracle on the 4th of October 2006.

DB03 NULL DACL on Oracle Process in Windows

The Oracle process on Windows has a NULL Discretionary Access Control List. This means than anyone can use the OpenProcess() function to obtain a handle to the process. This handle can then be used to open threads in the process, using OpenThread() and then using SetThreadContext() it is possible to redirect the path of execution by setting the value of the EIP register. The process also has a number of shared memory sections with NULL DACLs – these can be used as locations to inject shellcode. As Oracle running on Windows runs with SYSTEM privileges an attacker can run code at this level and gain complete control of the server. This flaw was fully discussed in the Oracle Hacker's Handbook and was reported to Oracle on the 5th June 2005. It should also be noted that Cesar Cerrudo independently discovered the same flaw.

Refs:
http://www.freelists.org/archives/oracle-l/12-2006/msg00004.html

https://www.blackhat.com/presentations/bh-dc-07/Cerrudo/Presentation/bh-dc-07-Cerrudo-ppt.pdf

DB04 PL/SQL Injection in DBMS_AQADM_SYS
The DBMS_AQADM_SYS package owned by SYS contains a number of PL/SQL Injection flaws. These were reported to Oracle by Alex Kornbrust on 1st November 2005.

Refs:
http://www.red-database-security.com/advisory/oracle_sql_injection_dbms_aqadm_sys.html

DB05 AUTH_ALTER_SESSION After Logon Trigger Bypass
When a user authenticates they supply some SQL to alter the session. This SQL can be anything however and executes before after logon triggers execute. This can be abused by attackers with a valid user ID and password to potentially bypass security policies. This flaw relates to an issue discovered by Imperva in October 2005 – see references. I reported this particular issue to Oracle on the 19th December 2006 but it seems that Alex Kornbrust also reported it as well on the 7th June 2006.

Refs:
http://www.red-database-security.com/advisory/bypass_oracle_logon_trigger.html
http://www.imperva.com/application_defense_center/papers/oracle-dbms-01172006.html

DB06 SQL Injection Flaw in DBMS_APPLY_USER_AGENT
The DBMS_APPLY_USER_AGENT package owned by SYS contains a procedure called SET_REGISTRATION_HANDLER. This procedure takes as its second argument the name of a function and passes it to DBMS_APPLY_ADM_INTERNAL.ALTER_APPLY procedure. This flaw was discovered by Paul Wright and reported to Oracle on the 22nd of March 2006.

DB07 SQL Injection Flaw in DBMS_UPGRADE_INTERNAL
The DBMS_UPGRADE_INTERNAL package owned by SYS contains a number of SQL injection flaws. These were reported to Oracle by Alex Kornbrust on the 1st November 2005.

Refs:
http://www.red-database-security.com/advisory/oracle_sql_injection_dbms_upgrade_internal.html

EM01 Authentication Bypass in Intelligent Agent
The Oracle Intelligent Agent gathers performance information about the server. It is possible to use the services provided by the agent and shut it down without authentication. I reported this to Oracle on the 8th of June 2004.

DB08 Buffer Overflow in DBMS_CDC_IPUBLISH
The DBMS_CDC_IPUBLISH package owned by SYS contains a procedure called CHGTAB_CACHE. This procedure is vulnerable to a stack based buffer overflow and is triggered by passing an overly long CHANGE_TABLE_NAME parameter. I reported this overflow to Oracle on the 8th of June 2005.

DB09 SQL Injection in DBMS_CDC_PUBLISH
The DBMS_CDC_PUBLISH packages calls java classes in CDC.jar. Some of these classes are vulnerable to SQL injection and are discussed in the Oracle Hacker's Handbook. Both the October 2006 and January 2007 Critical Patch Updates addressed some of these issues – this patch completes the process.

Refs:
http://www.databasesecurity.com/oracle/OracleOct2006-CPU-Analysis.pdf

The following issues are listed as having zero risk under CVSS.
DB10 Buffer Overflow in DBMS_SNAP_INTERNAL
The patch contains an updated kkzi.o object file.
DB11 Flaw in genezi utility

DB12	**Flaw in ctxsrv server daemon (command line)**
DB13	**Flaw in mig utility**

An NGSSoftware Insight Security Research (NISR) Publication

[**http://www.ngssoftware.com/**](http://www.ngssoftware.com/)