Härtung von Oracle12c Release 1 & 2 Datenbanken

Norbert Debes
Externer Datenbankadministrator
Deutsches Patent- und Markenamt, München

Industriespionage

DOW JONES, A NEWS CORP COMPANY

DJIA ▲ 21809.29 0.26% | S&P 500 ▲ 2460.73 0.12% | Nasdaq ▼ 6362.20 -0.21% | U.S. 10 Yr ▼ 0/32 Yield 2.060% | Crude Oil ▲ 49.17 1.05% | Euro ▲ 1.1944 0.24%

THE WALL STREET JOURNAL.

Subscribe Now | Sign In

SPECIAL OFFER: JOIN NOW

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate Search

BUSINESS

Lockheed Martin Hit By Security Breach

By Nathan Hodge And Ian Sherr

Updated May 27, 2011 10:34 p.m. ET

Hackers may have infiltrated the networks of top U.S. weapons manufacturer Lockheed Martin Corp., according to a person with knowledge of the attacks.

uters, prompted

ely clear if any

WELT N24 DIGITAL ZEITUNG TV

HOME LIVE TV MEDIATHEK POLITIK WIRTSCHAFT SPORT MEHR ABO

HOME » NEWSTICKER » NEWS1 (AFP - JOURNAL) » Internet: Wikileaks: CIA-Hacker operieren vom US-Konsulat in Frankfurt aus

NEWSTICKER

NEWS1 (AFP - JOURNAL) INTERNET

Wikileaks: CIA-Hacker operieren vom US-Konsulat in Frankfurt aus

Veröffentlicht am 07.03.2017 | Lesedauer: 2 Minuten

Wikileaks-Gründer Julian Assange

Quelle: AFP/Archiv/BEN STANSALL

cle12c Relea

Handelsblatt

DIGITALPASS 4 WOCHEN GRATIS TESTEN

NEUE STUDIE

Spionage kostet deutsche Wirtschaft Milliarden

Datum: 19.02.2017 16:11 Uhr

Ausländische Geheimdienste spionieren in deutschen Firmen. Das geht aus geheimen NSA-Dokumenten hervor, die Edward Snowden veröffentlicht hat. Die Unternehmen kostet das ein Vermögen.

Facebook Twitter Google+ Xing Linkedin

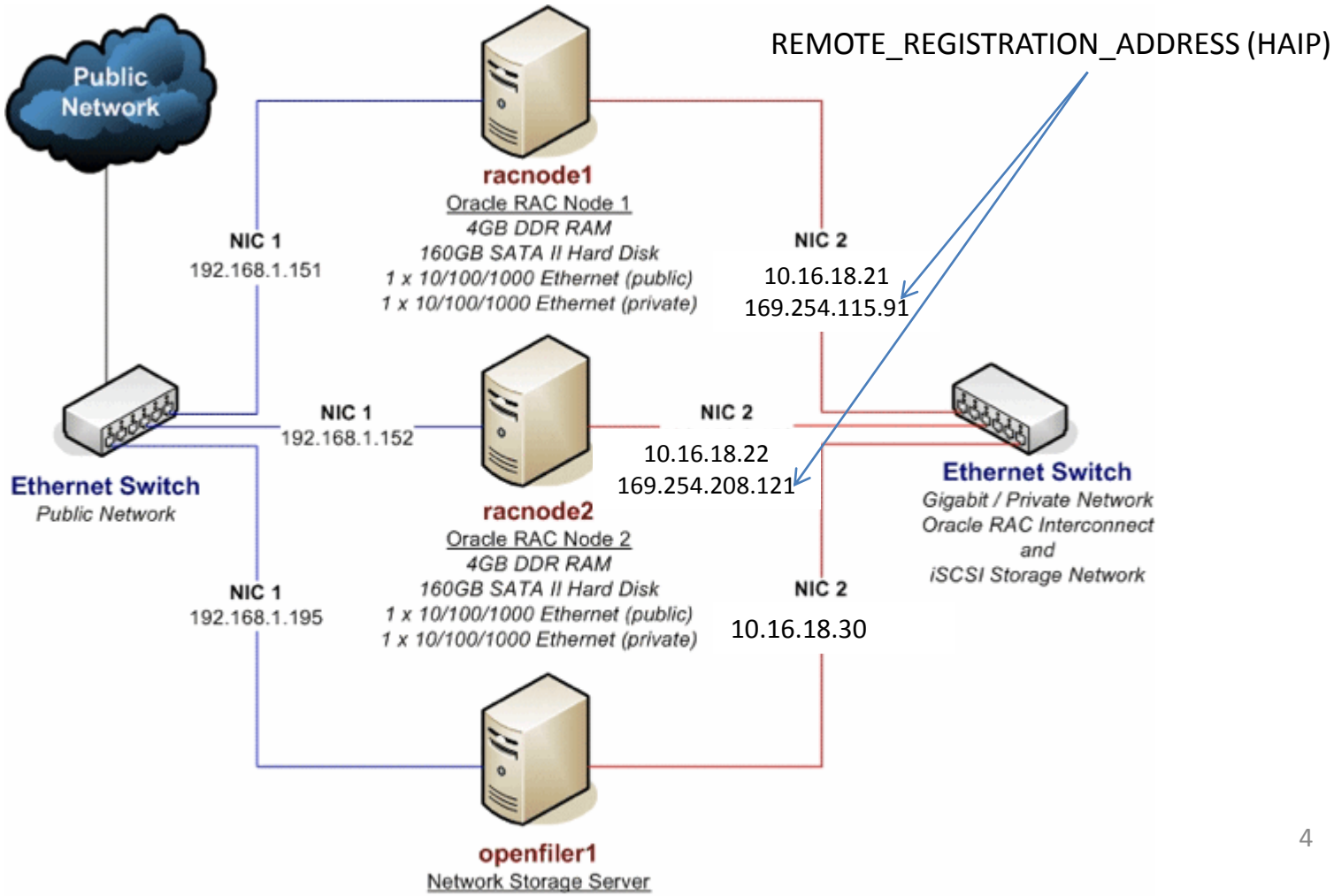
0

6

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

- Regression: Bug 24462646: "AFTER UPG GI FROM 11.2, AGENT NOT SET REMOTE_REGISTRATION_ADDRESS TO SCAN LSNR"
- Oracle RAC 12cR1 und 12cR2 sind angreifbar, falls Netzwerkpakete aus dem öffentlichen Netz eine HAIP des Interconnects im Netz 169.254.0.0/16 erreichen können (arp_ignore).
- Bug 26739452: Oracle Restart 12cR1 und 12cR2 sind wegen der Einstellung VALID_NODE_CHECKING_REGISTRATION_LISTENER = SUBNET angreifbar (REMOTE_REGISTRATION_ADDRESS=OFF)

HAIP (link-local Netz 169.254.0.0/16)



Gefährliches "Saatgut"

- Privilegieneskalation über funktionsbasierten Index
  - „Litchfield found the flaw while conducting security tests for a client and initially suspected it to be a backdoor left behind by an attacker.”
  - Litchfield feels there is "absolutely no good reason" for Oracle to have granted PUBLIC the INDEX privilege on the DUAL table
  - “Litchfield said Oracle told him it had no record of why the backdoor existed”
  - https://www.theregister.co.uk/2015/01/20/oracle_readies_to_patch_gobsmacking_vulnerability_tomorrow/

JServer

- 12c: Ausführung beliebiger SQL Anweisungen mittels DBMS_SQL and DBMS_JAVA_TEST
  - Litchfield: “If Java is not actively being used by the database’s applications it should be removed. This prevents this attack and also addresses many more security issues by reducing attack surface”
  - http://www.davidlitchfield.com/Exploiting_PLSQL_Injection_on_Oracle_12c.pdf

INHERIT PRIVILEGES

- Neuer Schutz vor Privilegieneskalation ab 12cR1
- REVOKE INHERIT PRIVILEGES ON USER <invoker> FROM PUBLIC;
- GRANT INHERIT PRIVILEGES ON USER <invoker> TO <IR owner>;
- Vergabe von INHERIT PRIVILEGES an ein PL/SQL Objekt über eine Rolle statt an gesamtes Schema ist nicht möglich

Oracle Home ohne Schreibrechte

- Höchste Sicherheit gegen Manipulationen im Installationsverzeichnis (mount -o ro)
- Schreibrecht u.a. in <OH>/dbs und <OH>/rdbms/audit bzw. log notwendig
- Symbolic Links auf Verzeichnisse mit Schreibrecht sind möglich
- LVM: zusätzliche Logical Volumes mit kleinen Dateisystemen
- Ohne LVM: Dateien mit kleinen Dateisystemen und Loopback-Mount

Absicherung von glogin.sql

- Sowohl glogin.sql als auch login.sql sind Angriffziele (z.B. per DBMS_ADVISOR.CREATE_FILE)
- Dateisystem ohne Schreibrecht:

```
# dd if=/dev/zero of=/usr/local/glogin_ro bs=1048576 count=10
# mke2fs -qF /usr/local/glogin_ro
# mount -o loop /usr/local/glogin_ro $ORACLE_HOME/sqlplus/admin
# echo 'set sqlprompt "&_USER.@&_CONNECT_IDENTIFIER> "' >>
   $ORACLE_HOME/sqlplus/admin/glogin.sql
# mount -o remount,ro /u01/app/product/gi/12.2/sqlplus/admin
```

- Automatischer Mount:

```
# tail -2 /etc/fstab
/usr/local/glogin_ro    /u01/app/product/gi/12.2/sqlplus/admin  ext2
   ro,loop
/usr/local/glogin_ro    /u01/app/product/rdbms/12.2/sqlplus/admin
   ext2    ro,loop
```

GRANT EXECUTE TO PUBLIC

- Viele Sicherheitsrichtlinien empfehlen REVOKE auf ca. 30 Packages
- Aber: Wie viele Packages enthalten bisher nicht entdeckte Sicherheitslücken?
- Konsequenz: Keine GRANTs an PUBLIC außer auf DUAL
- Technisch unproblematisch: Reine Fleißarbeit
- Aber: Upgrade bzw. Installationsskripte vergeben die GRANTs erneut

Grid Infrastructure

- Schutz der Automatic Storage Management (ASM) disk groups durch ASM Filter Driver (ASMFD)
  - Zugriffe durch Fremdprogramme werden unterbunden
  - Migration von ASMLib und udev zu ASMFD einfach möglich (Schalter --migrate)
- Kernel Modul: oracleafd (lsmod)

ASMFD (ASM Filter Driver)

- **Keine Rechte auf den Gerätedateien für Grid Infrastructure Software Owner**

```
$ ls -l /dev/xvdc1 /dev/xvdd1
brw-rw---- 1 root disk 202, 33 Oct  9 12:37 /dev/xvdc1
brw-rw---- 1 root disk 202, 49 Oct  9 12:37 /dev/xvdd1
$ head /dev/oracleafd/disks/* # plain text files
==> /dev/oracleafd/disks/XVDC1 <==
/dev/xvdc1

==> /dev/oracleafd/disks/XVDD1 <==
/dev/xvdd1
```

ASMFD (ASM Filter Driver)

```
$ asmcmd afd_state
ASMCMD-9526: The AFD state is 'LOADED' and filtering is 'ENABLED' on host
   'test3.dpma.de'
$ asmcmd afd_lsdsk
--------------------------------------------------
Label                     Filtering   Path
==================================================
XVDC1                       ENABLED   /dev/xvdc1
XVDD1                       ENABLED   /dev/xvdd1
SQL> SELECT label, header_status, library
FROM v$asm_disk;
LABEL  HEADER_STATUS LIBRARY
------ ------------ ----------------------------------------
XVDC1  MEMBER       AFD Library - Generic , version 3 (KABI_V3)
XVDD1  MEMBER       AFD Library - Generic , version 3 (KABI_V3)
```

Deaktivierung / AS SYSDBA

```
$ cd $ORACLE_HOME/rdbms/lib
$ egrep 'dba_string:|DBA_GRP "' config.c
.Ldba_string:     .string ""
#define SS_DBA_GRP ""
$ rm config.o; make -f ins_rdbms.mk $PWD/config.o ioracle
$ srvctl start instance -db ORA122 -node `hostname`
$ egrep 'PRIVILEGE|ACTION'
   ORA1221_ora_27414_20170825161817695716143795.aud|head -59|tail -2
ACTION :[55] 'ALTER DATABASE OPEN /* db agent *//* {1:55751:11094} */'
PRIVILEGE :[6] 'SYSRAC'
SQL> CONNECT / AS SYSDBA
ERROR:
ORA-01017: invalid username/password; logon denied
SQL> CONNECT / AS SYSRAC
Connected.
SQL> SELECT open_mode FROM v$database;
OPEN_MODE
--------------------
READ WRITE
```

Berechtigungen von SYSRAC

```
SQL> SELECT * FROM session_privs ORDER BY 1;

PRIVILEGE
----------------------------------------
ALTER DATABASE
ALTER SESSION
ALTER SYSTEM
CREATE EVALUATION CONTEXT
CREATE RULE
CREATE RULE SET
DEQUEUE ANY QUEUE
ENQUEUE ANY QUEUE
MANAGE ANY QUEUE
SYSRAC

10 rows selected.
```

SYSRAC Rollen

```
SQL> SELECT * FROM session_roles ORDER BY 1;

ROLE
------------------------------------
AQ_ADMINISTRATOR_ROLE
```

Datapatch ohne Betriebssystemauthentifizierung

- Bug 18361221 : DATAPATCH FAILS WITH ORA-01017, AS IT CONNECTS DB ONLY USING OS AUTHENTICAITION
- Fixed in 12.2

```
$ ./datapatch -userid SYS # undocumented switch -userid
SQL Patching tool version 12.2.0.1.0 Production on Tue
   Aug 29 13:23:32 2017
...
Enter password for SYS:
Connecting to database...OK
...
Patch installation complete.  Total patches installed: 1
```

Multitenant Option

- LOCKDOWN PROFILE in 12c Release 2
- Abschalten von Merkmalen, Optionen, SQL-Anweisungen
- Multitenant Option: Kostenlos mit Single-Tenant Konfiguration

```
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

- Härtung TNS Listener
- Advanced Security für verschlüsselten Netzwerkverkehr von Oracle Net
- Passwortkomplexität (catpvf.sql in 12cR2)
- Auditing
- Rolle DBA
- Temporäre statt dauerhafte CREATE-Berechtigungen
- Setuid Programme
- External Jobs

Fragen?