iSeries DB2 stored procedures vulnerability

Summary

DB2 UDB for iSeries supports stored procedures calls. It also allows the CREATE PROCEDURE statement to reference existing program objects. Unfortunately, it does not require explicit definition of existing program objects as stored procedures, allowing the execution of ANY program via remote SQL calls. The SQL commands can be run against an AS400 ODBC, JDBC, DRDA or OLE DB connection. An active account on the iSeries is required for a successful exploit.

Bypass "Limited capability user" definitions

You still need an active account to log in, but this method can be used to execute commands that are otherwise blocked to a limited user. The iSeries contains a system program, QCMDEXC, that effectively provides a remote shell for command execution, similar to the SQL server xp_cmdshell procedure. With proper parameters, this program can be called to execute local commands.

After an ODBC connection is established with the DB2 AS400 database, we can first make sure that QCMDEXC was not declared as a stored procedure.

```
select * from sysprocs where upper(routine_name) = 'QCMDEXC'
```

Usually, an empty result set will be returned. To further test the QCMDEXC utility, we will do something benign, like create a message queue called "hack" on the server, and send a test message to this message queue.

```
Call qcmdexc('crtmsgq hack' , 0000000012.00000)
Call qcmdexc('sndmsg ''hacked you'' hack' , 0000000024.00000)
```

These lines call for some explanation. The QCMDEXC program requires 2 input parameters: a quoted string containing the command to execute, and a packed decimal number with a specific precision containing the exact string length. To make the iSeries auto-convert our manual value of 12 into the required precision, we must provide it with a string matching the precision requirements. Because the requirement is DECIMAL(15,5), the number must have exactly 10 significant digits with leading zeros, a decimal period, and exactly 5 zeros.

ANY iSeries program can be properly supplied with parameters and executed in this way.

Execute REXX scripts

The iSeries contains a system program, QREXX, that provides an API for executing REXX scripts on the server. With proper parameters, this program can be called to execute existing REXX scripts on the server. For example, if there is a REXX script called "DAILY" in file QREXSRC in library QGPL, then the following SQL call will execute it.

```
CALL QREXX ('DAILY     ', 'QREXSRC   QGPL      ', 0, '', '', 0)
```

Notice the padding with blanks. It is not necessary for stored procedures, but these programs are not declared as stored procedures and must be supplied with parameters having the exact length.

A user can create new programs and new REXX scripts

CL programs sources are kept in Source files (typically QCLSRC). REXX scripts are kept in Source files (Typically QREXSRC). Source files are accessible by SQL to modify, create and delete. An attacker can issue a stream of INSERT statements to a CL source file, and then compile it using the QCMDEXC shell. An attacker can issue a stream of INSERT statements to a REXX source file, and execute them using either QREXX, or the STRREXPRC command by QCMDEXC. Of course, source files also contain RPG, COBOL, and C programs, so an attacker can actually upload any program source to the server, compile it and run it. Let's see an example REXX script created.

```
Call qcmdexc('crtsrcpf qgpl/qsrcrex2' , 0000000022.00000)

Call qcmdexc('addpfm rexxhack qgpl/qsrcrex2' , 0000000030.00000)

Create alias qgpl/rexxhack qgpl/qsrcrex2(rexxhack)

Insert into qgpl/rexxhack (srcseq, srcdta) values(1, '/* this is a
rexx script */')

Insert into qgpl/rexxhack (srcseq, srcdta) values(2, 'ADDRESS
COMMAND')

Insert into qgpl/rexxhack (srcseq, srcdta) values(3, 'line=''sndmsg
rexx hack'''')

Insert into qgpl/rexxhack (srcseq, srcdta) values(4, 'interpret
line')

Insert into qgpl/rexxhack (srcseq, srcdta) values(5, 'return')

CALL QREXX ('rexxhack  ', 'QSRCREX2  QGPL      ', 0, '', '', 0)
```


CL command and REXX scripts can be used on their own to gain further access to the server and database, or as a tool to download additional programs or scripts via FTP and other tools.

The programs can be called by any database tool, including IBM's own Operations Navigator. Of course, a program can be written using the language of your choice to demonstrate the same.

Countermeasures

Revoke Public authority to all *PGM objects in the system, unless you intend them to be called from SQL.

Revoke Public authority to QCMDEXC and QREXX, if possible.

A security package that monitors SQL exit programs may work, but only for the IBM supplied ODBC driver, and will not work for DRDA access.

Summary

Any existing iSeries program can be executed by ODBC/JDBC, including command shells that can be used to execute system commands.

Vulnerable systems: OS/400 versions 3.2 - 5.3

References

http://www.securiteam.com/securitynews/5DP071F8VO.html

http://publib.boulder.ibm.com/iseries/v5r2/ic2924/index.htm?info/sqlp/rbafymst202.htm

More information about AS/400 vulnerabilities and about AS/400 security issues can be found in the "Hacking iSeries" book, at www.venera.com