

# [NEWS] Multiple IBM DB2 Vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0041.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 01/09/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 9 Jan 2005 19:15:05 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Multiple IBM DB2 Vulnerabilities

---

## SUMMARY

<<http://www-306.ibm.com/software/data/db2/>> IBM's DB2 database server contain several vulnerabilities in its that can be used to read and write files on the system, crash the server and run arbitrary machine code.

## DETAILS

Vulnerable Systems:

- \* DB2 v7.x

- \* DB2 v8.1

IBM DB2 db2fmp buffer overflow:

IBM's DB2 database server suffers from a local attack whereby passing an overly parameter to the db2fmp binary will overflow a stack based buffer.

db2fmp is used for running fenced libraries. A fenced library is one that is not loaded into the main DB2 process so in the event of an error the server is not taken down as well. On UNIX based versions of DB2, db2fmp is installed setuid root. Exploiting this buffer overrun can allow a local attacker to gain root privileges.

Note – Some versions may drop root privileges before the overflow can be

## Securiteam: [NEWS] Multiple IBM DB2 Vulnerabilities

exploited.

Note – Whilst the overflow is present on Windows platforms it cannot be exploited to gain elevated privileges.

IBM DB2 libdb2.so buffer overflow

libdb2.so.1, one of the libraries supplied with IBM's DB2 database server suffers from a buffer overflow vulnerability.

This vulnerability can be divided into two separate issues.

Firstly, when libdb2.so is loaded it reads the DBLPORT environment variable and copies the value to a buffer in the .bss section. This buffer is overflowed. By providing an overly long DB2LPORT environment variable it fills the db2MLNPort\_name buffer in the .bss section of libdb2.so.1 – then spills over into the db2node\_name buffer, into the instprof\_path buffer, into the instance\_path buffer and so on all the way into the install\_path buffer.

Secondly, when the sqloInstancePath() reads the install\_path we overflow a local stack based buffer of sqloGetInstancePath().

This can be exploited to gain root privileges. For example, db2cacpy is setuid root. This program loads the library and calls sqloInstancePath() overflowing the buffer.

IBM DB2 call buffer overflow:

IBM's DB2 database server suffers from a stack based buffer overflow vulnerability when using "call".

Under DB2 it is possible to load a library directly and execute a function:

call libname!function

By passing an overly long libname it is possible to overflow a stack based buffer and overwrite the saved return address. When exploited this can allow an attacker to gain elevated privileges.

Note 1) if an attacker can place an arbitrary library on the system (and there are ways to do this via DB2 and SQL) then there is no need to exploit this overflow. It is sufficient simply to create the library and export a function that takes no parameters.

Note 2) "CREATE WRAPPERS" uses the same code as "CALL" and is presents another vector.

IBM DB2 JDBC Applet Server buffer overflow:

IBM's DB2 JDBC Applet Server suffers from a stack based buffer overflow vulnerability that can be exploited remotely without a user ID or password.

When a client connects to the JDBC applet server on TCP port 6789 it does so using a proprietary protocol. The connection packet starts with ValidDb2jdTokenFromTheClientSide and includes the username, the password,

## Securiteam: [NEWS] Multiple IBM DB2 Vulnerabilities

the db2java.zip version and the database to connect to.

The problem arises as follows:

First, an attacker attempts to authenticate to the JDBC applet server on TCP 6789 with an overly long username of c. 2200 bytes then disconnects gracefully.

Second, they reconnect, but this time send a short username but set the db2java.zip version to something other than expected by the server. Set the version to c. 544 Unicode bytes \x00\x41.

An error is logged and at some stage the null terminator is removed and the original username that was sent is concatenated to the db2java.zip version.

This is then copied to a stack based buffer and it overflows.

IBM DB2 SATADMIN.SATENCRYPT buffer overflow:

IBM's DB2 database server, when configured for Satellite Administration includes a number of SQL functions. One of these, the SATENCRYPT function suffers from a stack based buffer overflow vulnerability.

The SATENCRYPT function in the SATADMIN schema is vulnerable to a classic stack based overflow. The satencrypt function is exported by db2prom.dll and one of it's subfunctions creates a 40 byte buffer. User supplied data is copied to the buffer until a null terminator is reached in a while loop. By passing a parameter longer than 40 bytes allows the attacker to overflow the buffer and overwrite the saved return address. By exploiting this an attacker can gain elevated privileges.

Note – by default, public cannot execute this function.

IBM DB2 Windows Permission Problems:

Almost all shared memory sections and events in the Windows version of DB2 have weak permissions; all sections can be read and written by Everyone, and all events can be set and waited on by Everyone. This results in a number of security issues relating to the privileges of local users.

\* Depending on the server's authentication mode, any user can read plaintext windows usernames and passwords from the 'DB2SHMSECURITYSERVICE' section. If the authentication mode is 'client', the username and password combinations for all client connections can be read from this section. The data in this section persists until another connection is made. Any user can shut down DB2, by setting the event named 'DB2SHUTDOWNSEM'+ pid, for example: DB2SHUTDOWNSEM000002ec

\* Any user can DOS the "DB2 Security Server", by writing non-zero values to the section 'DB2SHMSECURITYSERVICE', followed by setting the security service 'input' event, to make the service read the input data:

DB2NTSECURITYINPUT

The service will then crash.

## Securiteam: [NEWS] Multiple IBM DB2 Vulnerabilities

\* Any user can read potentially sensitive query and/or query result data from a number of shared memory sections. The following sections are marked readable by 'Everybody':

```
section read DB20QM
section read DB2GLBQ0QM
section read DB2SHMDB2_0APP
section read DB2SHMDB2_0APL00000003
section read DB2SHMDB2_0APL00000004
section read DB2SHMDB2_0APL00000005
..etc
```

\* After writing to the world-writeable section 'DB20QM':

```
section write DB20QM
.. the DB2 'command line processor' will not run, nor will the 'command
center', the server has effectively been DOSsed.
```

IBM DB2 to\_char and to\_date Denial Of Service:

IBM DB2 is vulnerable to Denial of Service conditions when processing to\_char and to\_date function calls.

\* If the to\_char function is called with an empty string for its second parameter, DB2 dereferences a null pointer and terminates:

```
select to_char('aaa',") from sysibm.sysdummy1
```

\* If the to\_date function is called with an empty string for its second parameter, DB2 dereferences a null pointer and terminates:

```
select to_date('aaa', ") from sysibm.sysdummy1
```

In both cases, DB2 must be restarted in order to restore normal functionality.

IBM DB2 XML functions overflows:

The xmlvarcharfromfile suffers from a buffer overflow vulnerability. When and only when, 94 bytes are supplied for the second argument a pointer to the user supplied string is written over the saved return address so when ucncv\_open\_2\_0 (in db2xmlfn.dll) returns – it does so into the string. This allows an attacker to run arbitrary code and elevate privileges.

The xmlclobfromfile, xmlfilefromvarchar and xmlfilefromclob functions are also vulnerable.

IBM DB2 XML Functions File Creation Vulnerabilities:

The XMLFileFromVarchar and XMLFileFromClob functions can be used to create files on the remote server. If the file exists the original is overwritten with the new content. The permissions of the account running DB2 is used and not that of the user. This vulnerability can be used to create executable binaries on the remote server as well. An attacker could create a library for example and then load it via "CALL".

The XMLVarcharFromFile and XMLClobFromFile can be used to read files from the remote server.

Fix Information:

IBM has published a patch and can be obtained with the latest fixpak.

Securiteam: [NEWS] Multiple IBM DB2 Vulnerabilities

<<http://www-306.ibm.com/software/data/db2/udb/support/downloadv8.html>>  
<http://www-306.ibm.com/software/data/db2/udb/support/downloadv8.html> – DB2  
v8.1

<<http://www-306.ibm.com/software/data/db2/udb/support/downloadv7.html>>  
<http://www-306.ibm.com/software/data/db2/udb/support/downloadv7.html> – DB2  
v7.x

The original articles can be found at:

- <<http://www.ngssoftware.com/advisories/db205012005A.txt>>
- <http://www.ngssoftware.com/advisories/db205012005A.txt>
- <<http://www.ngssoftware.com/advisories/db205012005B.txt>>
- <http://www.ngssoftware.com/advisories/db205012005B.txt>
- <<http://www.ngssoftware.com/advisories/db205012005C.txt>>
- <http://www.ngssoftware.com/advisories/db205012005C.txt>
- <<http://www.ngssoftware.com/advisories/db205012005D.txt>>
- <http://www.ngssoftware.com/advisories/db205012005D.txt>
- <<http://www.ngssoftware.com/advisories/db205012005E.txt>>
- <http://www.ngssoftware.com/advisories/db205012005E.txt>
- <<http://www.ngssoftware.com/advisories/db205012005F.txt>>
- <http://www.ngssoftware.com/advisories/db205012005F.txt>
- <<http://www.ngssoftware.com/advisories/db205012005G.txt>>
- <http://www.ngssoftware.com/advisories/db205012005G.txt>
- <<http://www.ngssoftware.com/advisories/db205012005H.txt>>
- <http://www.ngssoftware.com/advisories/db205012005H.txt>
- <<http://www.ngssoftware.com/advisories/db205012005I.txt>>
- <http://www.ngssoftware.com/advisories/db205012005I.txt>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nisr@nextgenss.com>>  
NGSSoftware Insight Security Research.

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
To unsubscribe from the list, send mail with an empty subject line and body to:  
[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)  
In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.  
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential,  
loss of business profits or special damages.