

# [NEWS] Multiple IBM DB2 Stack Overflow Vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0065.html>

---

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

**Date:** 09/18/03

To: list@securiteam.com

Date: 18 Sep 2003 18:37:48 +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 Stack Overflow Vulnerabilities

---

## SUMMARY

DB2 is IBM's relational database software, oriented toward the deployment and development of e-business, business intelligence, content management, and enterprise resource planning and customer relationship management solutions. DB2 can be deployed in AIX, HP-UX, Linux, Solaris, and Windows environments.

IBM's DB2 database ships with two vulnerable setuid binaries, namely db2licm and db2dart. Both binaries are vulnerable to a buffer overflow that allows a local attacker to execute arbitrary code on the vulnerable machine with privileges of the root user. The vulnerability is triggered providing a long command line argument to the binaries.

By default (in the environment available during research), the vulnerable binaries have the following privileges (for example in the case of db2licm):

```
-r-sr-x---- 1 root db2iadm1 31926 Jun 21 2002
/home/db2inst1/sqllib/adm/db2licm
-r-sr-x---- 1 root db2asgrp 31926 Jun 21 2002
/home/db2as/sqllib/adm/db2licm
```

## Securiteam: [NEWS] Multiple IBM DB2 Stack Overflow Vulnerabilities

The db2as is the only user of the db2iadm1 group, and db2inst1 is the only user of the db2asgrp group. Therefore, in a default install, an attacker with access to the system with any those accounts, will be able to escalate privileges to the root account.

### DETAILS

#### Vulnerable Packages:

- \* IBM DB2 Universal Data Base v7.2 for Linux/x86 is vulnerable.
- \* IBM DB2 Universal Data Base v7.2 for Linux/s390 is vulnerable.

Other IBM DB2 versions and target platforms were not available for testing, but may be vulnerable as well.

#### Solution/Vendor Information/Workaround:

The db2dart issue is fixed in Fixpak 10 for DB2 v7.2.

Fixpak 10 is available 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>

The db2licm issue is fixed in Fixpak 10a for DB2 v7.2.

Fixpak 10a will soon be available at:

<http://www-3.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/v7fphist.d2w/report>  
<http://www-3.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/v7fphist.d2w/report>

If Fixpak 10a is not already available in this webpage, you can download it from IBM's FTP site. For example the 32-bit Intel Linux version of fixpack 10a is located at:

[ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/db2linuxv7/FP10a\\_U495179](ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/db2linuxv7/FP10a_U495179)  
[ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/db2linuxv7/FP10a\\_U495179](ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/db2linuxv7/FP10a_U495179)

#### Technical Description – Exploit/Concept Code:

The following tests are enough to confirm a binary is vulnerable.

Executing these perl scripts should produce a segmentation fault in vulnerable binaries:

```
/home/db2as/sqllib/adm/db2dart `perl -e 'print "A"x1287`
```

Segmentation fault

```
/home/db2as/sqllib/adm/db2licm `perl -e 'print "A"x999`
```

..

User Response: Enter the name of a file that exists and can be opened and try the command again.

Segmentation fault

..

## Securiteam: [NEWS] Multiple IBM DB2 Stack Overflow Vulnerabilities

Both binaries suffer from a simple stack based buffer overflow. Exploitation of the vulnerabilities is trivial. To confirm the exploitability, sample exploit code was developed for DB2 7.1 binaries for the Linux operating system running on x86 and s390 systems.

### ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<<http://www.coresecurity.com/common/showdoc.php?idx=366&idxseccion=10>>  
<http://www.coresecurity.com/common/showdoc.php?idx=366&idxseccion=10>.

The information has been provided by Juan Pablo Martinez Kuhn from Core Security Technologies.

=====

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

In order to subscribe to the mailing list, simply forward this email to: 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.