

# [UNIX] IBM DB2 Universal Database DB2INSTANCE File Creation Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00084.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 26 Feb 2007 14:58:16 +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 Universal Database DB2INSTANCE File Creation Vulnerability

---

### SUMMARY

IBM Corp.'s <<http://ibm.com/db2/>> DB2 Universal Database product is a large database server product commonly used for higher end databases.

Local exploitation of a file creation vulnerability in IBM Corp.'s DB2 Universal Database could allow attackers to elevate privileges to the superuser.

### DETAILS

#### Vulnerable Systems:

- \* IBM Corp.'s DB2 Universal Database 9.1 release installed on Linux.
- \* Other versions are suspected to be vulnerable as well.
- \* This vulnerability does not affect DB2 Universal Database running on the windows platform.

This vulnerability exists due to unsafe file access from within several setuid-root binaries. Specifically, when supplying the DB2INSTANCE environment variable, the setuid-root DB2 administration binaries will use the home directory of the specified user for loading configuration data.

## [UNIX] IBM DB2 Universal Database DB2INSTANCE File Creation Vulnerability

This allows attackers create or append to arbitrary files by creating a specific executing environment. Additionally, the user's umask settings will be honored allowing the creation of root-owned world-writable files.

Successful exploitation allows a local attacker to gain root privileges.

It should be noted that the attacker does not appear to have a great deal of control over the contents of the data written. However, this does not significantly impact exploitation.

### Workaround:

The best defense against this type of vulnerability is to prevent untrusted users from having code execution abilities on the respective database server. The following workarounds also have value.

Use a more strict permissions setting for the DB2 instance directory would prevent non-instance users from accessing the setuid-root binaries.

Remove the setuid bit from all programs included with DB2.

These configuration changes have not been tested and may cause adverse behavior.

### Vendor Status:

IBM Corp. has addressed this vulnerability within IBM Universal Database DB2 9 Fixpack 2. For more information, consult the corresponding IBM APAR #IY94817 by visiting the following URL.

<<http://www-1.ibm.com/support/docview.wss?uid=swg21255745>>  
<http://www-1.ibm.com/support/docview.wss?uid=swg21255745>

### Disclosure Timeline:

- \* 11/15/2006 – Initial vendor notification
- \* 01/29/2007 – Initial vendor response
- \* 02/22/2007 – Coordinated public disclosure

## ADDITIONAL INFORMATION

The information has been provided by iDefense.  
The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=480>>  
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=480>

=====

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:

[UNIX] IBM DB2 Universal Database DB2INSTANCE File Creation Vulnerability

list-unsubscribe@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====  
=====

**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.