

# [Full-disclosure] iDefense Security Advisory 02.07.08: IBM DB2 Universal Database db2pd Arbitrary Library Loading Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-02/msg00109.html>

---

- *From:* iDefense Labs <[labs-no-reply@xxxxxxxxxxxxx](mailto:labs-no-reply@xxxxxxxxxxxxx)>
  - *Date:* Thu, 07 Feb 2008 17:05:53 -0500
- 

iDefense Security Advisory 02.07.08  
<http://labs.iddefense.com/intelligence/vulnerabilities/>  
Feb 07, 2008

## I. BACKGROUND

IBM Corp.'s DB2 Universal Database product is a large database server product commonly used for high end databases. For more information, visit the following URL.

<http://ibm.com/db2/>

## II. DESCRIPTION

Local exploitation of a library loading vulnerability in IBM Corp.'s DB2 Universal Database could allow attackers to gain root privileges.

When the DB2INSTANCE environment variable is set, the libdb2 library will use the corresponding user's directory in place of the DB2 instance directory. This allows an unprivileged local user to control the directory structure on which several set-uid root binaries operate.

This vulnerability exists due to the way the db2pd binary loads a library. The program will construct the path to a library to be loaded by concatenating the path to the instance directory with the static string `"/sqlib/lib/libdb2fmttmp.so"`. When an attacker sets the DB2INSTANCE environment variable to their user name, the binary will load the library from their directory.

## III. ANALYSIS

Exploitation allows local attackers to gain root privileges. In order to exploit this vulnerability, an attacker must be able to execute the set-uid root db2pd binary.

## IV. DETECTION

iDefense has confirmed the existence of this vulnerability in IBM Corp.'s DB2 Universal Database 9.1 with FixPack 2 installed on a Linux system. Other versions, including those for other UNIX systems, are also suspected to be vulnerable.

## V. WORKAROUND

In order to mitigate exposure to this vulnerability, implement one of the following workarounds.

Using strict permissions for the DB2 instance directory will prevent non-instance users from accessing the set-uid root binaries.

Remove the set-uid bit from the db2pd binary.

## VI. VENDOR RESPONSE

IBM Corp. has addressed these vulnerabilities by releasing V9 Fix Pack 4 and version V8 FixPak 16 of its Universal Database product. More information can be found at the following URLs.

V8: <http://www-1.ibm.com/support/docview.wss?uid=swg21256235>

V9: <http://www-1.ibm.com/support/docview.wss?uid=swg21255572>

## VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2007-5757 to this issue. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org/>), which standardizes names for security problems.

## VIII. DISCLOSURE TIMELINE

03/22/2007 Initial vendor notification  
03/23/2007 Initial vendor response  
11/13/2007 V9 Fix Pack 4 made available  
01/28/2008 V8 Fix Pack 16 made available  
02/05/2008 V8 Fix list made available  
02/07/2008 Public disclosure

## IX. CREDIT

The discoverer of this vulnerability wishes to remain anonymous.

Get paid for vulnerability research

<http://labs.idefense.com/methodology/vulnerability/vcp.php>

Free tools, research and upcoming events

<http://labs.idefense.com/>

## X. LEGAL NOTICES

Copyright © 2008 iDefense, Inc.

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express written consent of iDefense. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please e-mail customerservice@xxxxxxxxxxxxx for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>