

iDefense Security Advisory 02.22.07: IBM DB2 Universal Database Multiple Privilege Escalation Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-02/msg00445.html>

- *From:* iDefense Labs <labs-no-reply@xxxxxxxxxxxxx>
 - *Date:* Thu, 22 Feb 2007 19:10:34 -0500
-

IBM DB2 Universal Database Multiple Privilege Escalation Vulnerabilities

iDefense Security Advisory 02.22.07
<http://labs.iddefense.com/intelligence/vulnerabilities/>
Feb 22, 2007

I. BACKGROUND

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

II. DESCRIPTION

Local exploitation of a multiple vulnerabilities in IBM Corp.'s DB2 Universal Database allow attackers to cause a denial of service condition or elevate privileges to root.

Several vulnerabilities exist due to unsafe file access from within several setuid-root binaries. Specifically, when supplying certain environment variables, the DB2 administration binaries will use the specified filename for saving data. This allows an attacker to create or append to arbitrary files as root.

A heap-based buffer overflow vulnerability can occur when copying data from an environment variable. The variable contents are copied to a static BSS segment buffer without ensuring proper NUL termination. Consequently, this allows an attacker to cause a heap overflow in a later function call.

A stack-based buffer overflow can occur when an environment variable contains a long string. By specifying a specially crafted value, it is possible to overwrite the return address of a function and execute arbitrary code.

III. ANALYSIS

iDefense Security Advisory 02.22.07: IBM DB2 Universal Database Multiple Privilege Escalation Vulnerabilities

Successful exploitation allows a local attacker to cause a denial of service condition or potentially gain root privileges.

In some cases, the attacker does not appear to have any control over the contents of the data written to disk. If this is true, then privilege escalation could only occur via another bug where the existence of specially crafted file name allows code execution. Denial of service is trivial by writing to /etc/nologin or corrupting other system files.

IV. DETECTION

iDefense has confirmed the existence of these vulnerabilities within IBM Corp.'s DB2 Universal Database 9.1 release installed on Linux. Other versions, including those installed on other architectures, are suspected to be vulnerable as well.

These vulnerabilities do not appear to affect DB2 Universal Database running on the windows platform.

V. WORKAROUND

The best defense against these vulnerabilities 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.

VI. VENDOR RESPONSE

IBM Corp. has addressed this vulnerability within IBM Universal Database DB2 9 Fixpack 2. For more information, consult the corresponding IBM APAR #IY94833 by visiting the following URL.

<http://www-1.ibm.com/support/docview.wss?uid=swg21255747>

VII. CVE INFORMATION

A Mitre Corp. Common Vulnerabilities and Exposures (CVE) number has not been assigned yet.

VIII. DISCLOSURE TIMELINE

11/15/2006 Initial vendor notification

iDefense Security Advisory 02.22.07: IBM DB2 Universal Database Multiple Privilege Escalation Vulnerabilities

01/29/2007 Initial vendor response

02/22/2007 Coordinated public disclosure

IX. CREDIT

These vulnerabilities were discovered by Joshua J. Drake (iDefense Labs).

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 © 2007 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.