

[VulnWatch] iDefense Security Advisory 08.16.07: IBM DB2 Universal Database Multiple Untrusted Search Path Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-08/msg00016.html>

- *From:* iDefense Labs <labs-no-reply@xxxxxxxxxxxx>
 - *Date:* Thu, 16 Aug 2007 18:55:46 -0400
-

IBM DB2 Universal Database Multiple Untrusted Search Path Vulnerabilities

iDefense Security Advisory 08.16.07

<http://labs.iddefense.com/intelligence/vulnerabilities/>

Aug 16, 2007

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 multiple untrusted search path vulnerabilities in IBM Corp.'s DB2 Universal Database could allow attackers to elevate privileges to the superuser.

These vulnerabilities exist due to the execution of binaries or loading of libraries within untrusted paths. In each case, the path to a binary or library is generated based on an environment variable that is under attacker control. Additionally, the files to be executed or loaded are located in a directory under attacker control.

III. ANALYSIS

Exploitation allows local attackers to gain root privileges.

In cases where programs are executed, an attacker need only create a specially crafted environment and file structure. In cases where a library is loaded, creating a library containing a specially crafted initialization section is sufficient.

In order to exploit some of these vulnerabilities, the attacker must be

a member of the "db2grp1" or a group corresponding with an installed DB2 instance.

IV. DETECTION

iDefense confirmed the existence of this vulnerability in version 9.1 Fix Pack 2 of IBM Corp.'s DB2 Universal Database installed on a Linux system. All prior versions, as well as builds for other UNIX-based operating systems, are suspected to be vulnerable.

V. WORKAROUND

Setting more strict permissions on the DB2 instance directory can help mitigate some of these vulnerabilities. Removing the setuid-bit from all programs included with DB2 can also help mitigate exposure. Note, these configuration changes have not been thoroughly tested and may cause adverse behavior.

VI. VENDOR RESPONSE

IBM Corp. has addressed this vulnerability by releasing V9 Fix Pack 3 and version V8 FixPak 15 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-2007-4275 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

03/23/2007 Initial vendor notification

03/23/2007 Initial vendor response

08/16/2007 Coordinated 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 © 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.