

[UNIX] IBM DB2 Universal Database Multiple Privilege Escalation Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00085.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 26 Feb 2007 14:56:13 +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 Multiple Privilege Escalation Vulnerabilities

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

DETAILS

Vulnerable Systems:

- * 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.

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

[UNIX] IBM DB2 Universal Database Multiple Privilege Escalation Vulnerabilities

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.

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.

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.

Vendor Status:

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

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.

[UNIX] IBM DB2 Universal Database Multiple Privilege Escalation Vulnerabilities

The original article can be found at:

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=481>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=481>

=====

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@xxxxxxxxxxxxxxxx

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

=====

=====

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.