

Patch available for critical IBM DB2 Universal Database flaws

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-10/0017.html>

From: NGSSoftware Insight Security Research (*nistr_at_NEXTGENSS.COM*)

Date: 10/05/04

Date: Tue, 5 Oct 2004 15:15:52 +0100

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Researchers at NGSSoftware have discovered multiple critical/high risk vulnerabilities in IBM's DB2 Universal Database. Versions affected include

DB2 8.1 Fixpak 7 and earlier

IBM has updated Fixpak 6 and 7 to 6a and 7a to include fixes for these flaws. In all, 20 vulnerabilities, mostly remotely exploitable buffer overflows, have been addressed by the updates. The updated Fixpaks have just been released and can be downloaded from

<http://www-306.ibm.com/software/data/db2/udb/support/downloadv8.html>

The flaws fixed in these Fixpaks equate to NGSS BUGID 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 117, 118, 119, 120, 121 and 122 from the Vendor Notification Alerts –

<http://www.nextgenss.com/vna.htm>.

NGSSoftware are going to withhold details about these flaws for three months. Full details will be published on the 5th of January 2005. This three month window will allow DB2 database administrators the time needed to test and apply the Fixpak before the details are released to the general public. This reflects NGSSoftware's new approach to responsible disclosure.

NGSSQuirreL for DB2, NGSSoftware's advanced vulnerability assessment scanner and security manager for IBM DB2, has been updated to check for and positively identify these flaws in DB2 database servers on the network. More information about NGSSQuirreL for DB2 can be found at

<http://www.nextgenss.com/db2.htm>.

NGSSoftware Insight Security Research

<http://www.databasesecurity.com/>

<http://www.nextgenss.com/>

+44(0)208 401 0070

--

NTBugtraq Editor's Note:

NT-Bugtraq: Patch available for critical IBM DB2 Universal Database flaws

Want to reply to the person who sent this message? This list is configured such that just hitting --