

[UNIX] IBM DB2 Remote DoS during CONNECT processing

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00042.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 20 Dec 2006 16:35:57 +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 Remote DoS during CONNECT processing

SUMMARY

When connecting to a remote DB2 instance, the version 7 client typically sends a SQLJRA packet requesting start of the connection. If this SQLJRA packet is specially crafted, it can cause a DoS attack by crashing the DB2 instance. Altering a few bytes at specific offsets in the packet exposes multiple NULL/invalid pointer dereference bugs in the server code. For example, on Windows, if 0x00 is used at any of these offsets, the `sqlc_db2ra_as_con_database` function (from `DB2ENGN.DLL`) attempts to access NULL or invalid memory locations, causing an unhandled access violation (0xC0000005). This causes the DB2 instance to crash.

DETAILS

Vulnerable Systems:

- * All versions of IBM DB2 Database Server

A malicious CONNECT data stream sent to a DB2 server from V7 client may cause instance crash, resulting in a denial of service. Server crashes with the following stack trace back:

-----Frame----- -----Function + Offset-----

[UNIX] IBM DB2 Remote DoS during CONNECT processing

0x2022DF24
sqle_db2ra_as_con_database__FP17sqle_db2ra_commonP10sqle_db2raP1
0sqler_glob + 0x268 0x2022D7CC
sqle_db2ra_as_con_driver__FP17sqle_db2ra_commonP10sqle_db2raP10s
qler_glob + 0x2A4 0xDA3AF114 sqledDb2raServerDriver + 0x129C
0xDB3FF900 sqljsDriveRequests__FP13sqle_agent_cbP11UCconHandle +
0x134 0xDB3FC480 sqljsDrdaAsInnerDriver__FP17sqlcc_init_structb
+ 0x2B4 0xDB3FBF60 sqljsDrdaAsDriver__FP17sqlcc_init_struct +
0x10C 0x200464EC sqleRunAgent__FPcUI + 0x578 0xD9598398
sqloCreateEDU__FPFPcUI_vPcUIP13SQLO_EDU_INFOP1 + 0x304
0xD9597EF8 sqloSpawnEDU + 0x4CC

Fix:

To fix the problem apply the fixpak 13 for DB2 version 8.1 (same as 8.2
FP6)

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

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4257>>
CVE-2006-4257

ADDITIONAL INFORMATION

The information has been provided by <<mailto:shatter@xxxxxxxxxxxxxx>> Team
SHATTER.

The original article can be found at:

<<http://www.appsecinc.com/resources/alerts/db2/2006-09-05.shtml>>
<http://www.appsecinc.com/resources/alerts/db2/2006-09-05.shtml>

=====

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@xxxxxxxxxxxxxx

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

=====
=====

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.