

[Full-disclosure] Details for BID 18428

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-09/msg00070.html>

- *From:* "Amichai Shulman" <shulman@xxxxxxxxxxxx>
 - *Date:* Wed, 6 Sep 2006 17:37:21 +0300
-

DB2 UDB – Unauthenticated Buffer Overflow and DoS (BID 18428)

Background

DB2 Universal Database (UDB)(tm) is a popular database software package from IBM available for legacy platforms as well as open systems (Unix and Windows). Clients use a protocol called DRDA to communicate with the DB2 UDB server. Protocol messages are used for session setup, authentication and data transfer

Scope

Imperva's Application Defense Center is conducting an extensive research of the DRDA protocol and its implementation. As part of the research the team has identified severe vulnerability in DB2 UDB's connection establishment mechanism that allows an attacker to terminate the UDB service, effectively denying service from all database users.

Findings

An attacker can send a specially crafted EXCSAT command during the handshake process with the server, causing the server process to crash. It seems that the command invokes a buffer overflow condition on the server possibly allowing execution of arbitrary code on the server.

Details

The first message used by a client when establishing a connection to the database is the EXCSAT message (message code 0x1041). This message includes an object called MGRLVLLS (code 0x2114) which in term contains a vector of 4 byte entries (two bytes for the manager code and two byte

[Full-disclosure] Details for BID 18428

for the compatibility level). When the size of the MGRLVLLS message is large enough a buffer overflow condition is invoked.

If the client terminates the connection immediately after sending this message the server process is terminated.

Exploit

Create an EXCSAT message with a very long (>1Kbytes) MGRLVLLS message. (see attached)

Tested Versions

Vulnerable

DB2 UDB version 8.x all platforms

Not Vulnerable

Vendor's Status

Vendor notified on Feb-8, 2006.

Vulnerability patched in UDB 8.x FixPak 12 on May 5th 2006, APAR is IY84096

Reported by vendor to Bugtraq on June 14th 2006 and labeled BID 18428

Workaround

None

Amichai Shulman
CTO

<<http://www.imperva.com/>> Imperva, Inc.

[Full-disclosure] Details for BID 18428

12 Hachilazon St.
Ramat Gan
Israel

(972) 3-6120133 x103 Office
(972) 54-5885083 Mobile
(972) 3-5711133 Fax
shulman@xxxxxxxxxxx

...