

Team SHATTER Security Advisory: Multiple DoS in JAR files manipulation procedures

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-04/msg00224.html>

- *From:* Team SHATTER <shatter@xxxxxxxxxxxxxx>
 - *Date:* Fri, 18 Apr 2008 11:19:38 +0100
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Team SHATTER Security Advisory

Multiple DoS in JAR files manipulation procedures

April 17th 2008

Risk Level:
High

Affected versions:
All versions of IBM DB2 Database Server on Windows platform.

Remote exploitable:
Yes (Authentication to Database Server is needed)

Credits:
These vulnerabilities were discovered and researched by Ariel Sanchez of Application Security Inc.

Details:
DB2 has multiple vulnerabilities which can lead to Denial of Service (DoS) attacks against the instance. When RECOVERJAR and REMOVE_JAR procedures are called with a specially crafted parameter the DB2 instance crashes. Any DB2 database user can exploit these vulnerabilities since PUBLIC permissions are granted to both procedures by default. The RECOVERJAR and REMOVE_JAR procedures are installed by default.

Impact:
Any remote authenticated attacker can crash the DB2 instance.

Vendor Status:
Vendor was contacted and a patch was released.

Fix:

Team SHATTER Security Advisory: Multiple DoS in JAR files manipulation procedures

To fix the problem apply the FP16(v8), FP4a(v9.1) and FP1(v9.5):

<http://www-1.ibm.com/support/docview.wss?rs=71&uid=swg21256235>

<http://www-1.ibm.com/support/docview.wss?rs=71&uid=swg21255572>

<http://www-1.ibm.com/support/docview.wss?rs=71&uid=swg21287889>

APAR:

IZ08945 – V8 FP16

IZ08512 – V9.1 FP4a

IZ15496 – V9.5 FP1

Timeline:

Vendor Notification – 9/11/2007

Vendor Response – 11/14/2007

Fix – 4/15/2008

Public Disclosure – 4/17/2008

Application Security, Inc's database security solutions have helped over 900 organizations secure their databases from all internal and external threats while also ensuring that those organizations meet or exceed regulatory compliance and audit requirements.

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.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.7 (MingW32)

iD8DBQFICHW59EOAcmTuFN0RAoXPAJ9XZYqIItRI//pNmMfIYO4TppUg6QCguSq3

ggtSxRqmxYVdZh7n1EMG2WA=

=VpBw

-----END PGP SIGNATURE-----