

# [NEWS] IBM DB2 Universal Database Administration Server Memory Corruption Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-02/msg00020.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 9 Feb 2008 10:52:49 +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 Administration Server Memory Corruption Vulnerability

---

### SUMMARY

IBM Corp.'s <<http://ibm.com/db2/>> DB2 Universal Database product is "a large database server product commonly used for high end databases. The DB2 Administration Server (DAS) provides functionality that implements the Java-based DB2 Control Center GUI". Remote exploitation of a memory corruption vulnerability within version 9.1 of IBM Corp.'s DB2 Universal Database Administration Server (DAS) allows attackers to crash the service or potentially execute arbitrary code in the context of the affected service.

### DETAILS

Vulnerable Systems:

\* DAS (db2dassrm) as included with DB2 9.1 with Fix Pack 2 for both Linux and Windows platforms

When handling certain remote administration requests, the Administration

## [NEWS] IBM DB2 Universal Database Administration Server Memory Corruption Vulnerability

Server uses a 32-bit pointer value supplied by the remote client. By supplying carefully chosen address values, an attacker can cause memory corruption or force the program to access invalid memory locations.

### Analysis:

Exploitation allows attackers to crash the service or execute arbitrary code within the context of the affected service. No authentication credentials are required. The attacker only needs the ability to establish a TCP session with the DAS on TCP port 523.

By default this service runs as "dasusr1" on Linux and "db2admin" on Windows. In the Linux version of the DAS, the process is monitored by a fault monitoring process and will restart automatically after a few seconds. This monitoring process does not exist in the Windows version.

### Workaround:

Employing firewalls to limit access to the affected service will mitigate exposure to this vulnerability.

### Vendor response:

IBM Corp. has addressed these vulnerabilities by releasing V9 Fix Pack 4 and V8 FixPak 16 of its Universal Database product. More information can be found at the following URLs:

\* V8: <<http://www-1.ibm.com/support/docview.wss?uid=swg21256235>>

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

\* V9: <<http://www-1.ibm.com/support/docview.wss?uid=swg21255572>>

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

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3676>>

CVE-2007-3676

### Disclosure timeline:

06/18/2007 – Initial vendor notification

06/20/2007 – Initial vendor response

08/14/2007 – V8 Fix Pack 15 made available

08/15/2007 – V9 Fix Pack 3 made available

10/10/2007 – V9 Fix Pack 3a made available

11/13/2007 – V9 Fix Pack 4 made available

01/28/2008 – V8 Fix Pack 16 made available

02/05/2008 – V8 Fix Pack 16 fix list made available

02/07/2008 – Public disclosure

### ADDITIONAL INFORMATION

The information has been provided by iDefense Labs.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=654>>

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=654>

=====

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@xxxxxxxxxxxxxxxxx

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

=====

=====

**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.