

# [UNIX] SAP MaxDB Signedness Error Heap Corruption Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00038.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 12 Mar 2008 11:40:34 +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>

-----

SAP MaxDB Signedness Error Heap Corruption Vulnerability

---

## SUMMARY

SAP's <<https://www.sdn.sap.com/irj/sdn/maxdb>> MaxDB is "a database software product. MaxDB was released as open source from version 7.5 up to version 7.6.00. Later versions are no longer open source but are available for download from the SAP SDN website (sdn.sap.com) as a community edition with free community support for public use beyond the scope of SAP applications. The "vserver" program is responsible for accepting and handling communication with remote database clients". Remote exploitation of a signedness error in the "vserver" component of SAP AG's MaxDB could allow attackers to execute arbitrary code.

## DETAILS

Vulnerable Systems:

\* SAP AG's MaxDB version 7.6.0.37 (on Linux)

After accepting a connection, the "vserver" process forks and reads parameters from the client into various structures. When doing so, it trusts values sent from the client to be valid. By sending a specially crafted request, an attacker can cause heap corruption. This leads to a

## [UNIX] SAP MaxDB Signedness Error Heap Corruption Vulnerability

potentially exploitable memory corruption condition.

### Analysis:

Exploitation allows an attacker to execute arbitrary code in the context of the running service. In order to exploit this vulnerability, an attacker must be able to establish a TCP session on port 7210 with the target host. Additionally, the attacker must know the name of an active database on the server.

Since this service uses the fork() system call once a connection has been accepted, an attacker can repeatedly attempt to exploit this vulnerability. Some exploitation attempts may result in the database process ceasing to run, in which case further exploitation attempts will not be possible.

### Vendor response:

SAP AG has addressed this vulnerability by releasing a new version of MaxDB. For more information, consult SAP note 1140135.

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0307>>  
CVE-2008-0307

### Disclosure timeline:

12/06/2007 – Initial vendor notification  
12/10/2007 – Initial vendor response  
03/10/2008 – Coordinated 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=669>>  
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=669>

=====

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@xxxxxxxxxxxxxxxx

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

=====

=====

### DISCLAIMER:

## [UNIX] SAP MaxDB Signedness Error Heap Corruption Vulnerability

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.