

# Multiple vulnerabilities in solidDB 06.00.1018

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-03/msg00350.html>

---

- *From:* Luigi Auriemma <[aluigi@xxxxxxxxxxxxx](mailto:aluigi@xxxxxxxxxxxxx)>
  - *Date:* Wed, 26 Mar 2008 21:29:48 +0100
- 

#####

Luigi Auriemma

Application: IBM solidDB

<http://www.solidtech.com/en/products/relationaldatabasemanagementsoftware/embed.asp>

Versions: <= 06.00.1018

Platforms: Windows (tested), Solaris, AIX, HP-UX and Linux

Bugs: A) format string in logging function

B) crash caused by arbitrary array index

C) NULL pointer

D) server termination through allocation error

Exploitation: remote

Date: 26 Mar 2008

Author: Luigi Auriemma

e-mail: [aluigi@xxxxxxxxxxxxx](mailto:aluigi@xxxxxxxxxxxxx)

web: [aluigi.org](http://aluigi.org)

#####

- 1) Introduction
- 2) Bugs
- 3) The Code
- 4) Fix

#####

- =====
- 1) Introduction
- =====

From vendor's website:

## Multiple vulnerabilities in solidDB 06.00.1018

"solidDB 6 is a relational database designed for fast, always-on access to data under high throughput conditions, to satisfy the real-time demands of communications platforms and applications. It includes both in-memory and on-disk engines, accessed by a single SQL interface."

This engine, originally developed by solid and now maintained by IBM, is also used in the products of various vendors.

#####

=====

### 2) Bugs

=====

#### ----- A] format string in logging function -----

The logging function used for keeping tracks of the various errors and operations (like wrong logins) is affected by a format string vulnerability exploitable for example using a malformed user or peer name.

#### ----- B] crash caused by arbitrary array index -----

A 32 bit number provided by the client is used on the server as an index for reading some values in an array, a too big number can be used to crash the server due to the access to invalid memory.

#### ----- C] NULL pointer -----

A NULL pointer vulnerability can be exploited through the sending of a specific type of packet.

#### ----- D] server termination through allocation error -----

A malformed packet can be used to terminate the server with the error message "Out of central memory" caused by the impossibility of allocating a certain amount of memory.

Multiple vulnerabilities in solidDB 06.00.1018

#####

=====  
3) The Code  
=====

<http://aluigi.org/poc/soliduro.zip>

#####

=====  
4) Fix  
=====

No fix

#####

---  
Luigi Auriemma  
<http://aluigi.org>