Bug Report - #001

Bug Information

**ID#:** 001 **Name:** Memset Error  
**Reporter:** Luke Collins **ION Version:** 3.6.2  
**Source code:** [Github Link](https://github.com/NASAHackTO/ion-dtn/blob/f1bb010a5e8fa01e5ef4b601222aa0242fe20c52/ion-open-source/ici/sdr/sdrxn.c)   
**Filename:** sdrxn.c **File Directory:** ‘ion-dtn/ion-open-source/ici/sdr/sdrxn.c’  
**Line:** 943

**Description:**At the beginning of line 927 of the ‘sdrxn.c’ a method called ‘static int createDbFile(SdrState \*sdr, char \*dbfilename)’ is declared. This method is responsible for creating database files and is the parent of many nested methods. Following this statement, a series of variables are declared that include a buffer of char data type and buffer size of long data type as depicted in *figure 1* below.

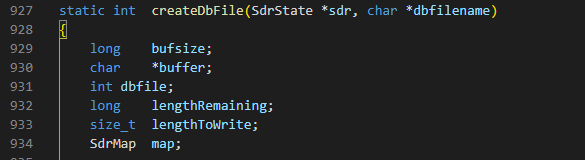


Figure 1: A screenshot of the initial declaration of the ‘createDbFile’ method and the aforementioned variables.

The C library function ‘**memset(void \*str, int c, size\_t n)’** copies the character **c** (an unsigned char) to the first **n** characters of the string pointed to, by the argument **str** and returns a pointer to the memory area str.

**Memset Parameters**

* **str** - *This is a pointer to the block of memory to fill.*
* **c -** *This is the value to be set. The value is passed as an int, but the function fills the block of memory using the unsigned char conversion of this value.*
* **n** - *This is the number of bytes to be set to the value.*

Given we attained the buffer variable of the char data type has a size of 1 byte. When looking at the use of the ‘**memset(buffer, 0 , sizeof(buffer)\*bufsize)**’ call in figure 2 below on line 943 we can see it is only writing a zero to the first byte of the memory area.

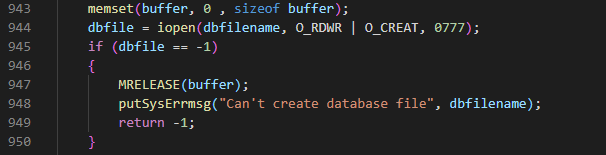


Figure 2: A screenshot of the initial use of the memset function along with the incorrect paraments.

The bug is minor and may not even pose any serious security issues but does suggest there could be further issues throughout the code.

Our suggested fix to the bug would be to multiply the buffer (1 byte) by bufsize (this size of the buffer) to ensure zero is written to every position.

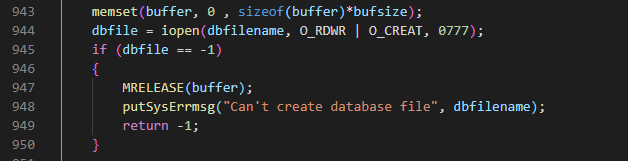


Figure 3: A screenshot of the correct implementation of memset.