| 1 void CWE190\_Integer\_Overflow\_\_int64\_t\_max\_preinc\_01\_bad() 2 { 3 int64\_t data; 4 data = 0LL; 5 /\* POTENTIAL FLAW: Use the maximum size of the data type \*/ 6 data = LLONG\_MAX; 7 { 8 /\* POTENTIAL FLAW: Incrementing data could cause an overflow \*/ 9 ++data; 10 int64\_t result = data; 11 printLongLongLine(result); 12 } 13 } |
| --- |

From the code at line 3, we can see that the variable “data” has a type of “int64\_t” (also known as “long long int”), whose value ranges from -2^31 to 2^31-1. The code at line 6 assigns LLONG\_MAX (i.e., 2^31-1 ) to “data” and then adds 1 to “data” at line 9, which goes beyond the maximal value of a “long long int” and overflows the value in “data”. Thus, an integer overflow happens.