Ticket Hash:	8f157e8010b22af03cb95f6e4f070fb4ccc07fcf		
Title:	Heap Buffer Overflow in multiSelectOrderBy		
Status:	Fixed	Type:	Code_Defect
Severity:	Minor	Priority:	Low
Subsystem:	Unknown	Resolution:	Fixed
Last Modified:	2020-06-15 13:56:11		
Version Found In:			

User Comments:

yongheng added on 2020-06-14 20:14:12:

```
Affect at least trunk and 3.32 release version.

POC:
---
CREATE TABLE a(b);
CREATE VIEW c(d) AS SELECT b FROM a ORDER BY b;
SELECT sum(d) OVER( PARTITION BY(SELECT 0 FROM c JOIN a WHERE b =(SELECT b INTERSECT SELECT d FROM c) AND b = 123)) FROM c;
---
```

---

drh added on 2020-06-15 13:56:11:

Simplified test case that does not involve window functions:

```
CREATE TABLE t1(c1);     INSERT INTO t1 VALUES(12),(123),(1234),(NULL),('abc');
CREATE TABLE t2(c2);     INSERT INTO t2 VALUES(44),(55),(123);
CREATE TABLE t3(c3,c4);  INSERT INTO t3 VALUES(66,1),(123,2),(77,3);
CREATE VIEW t5 AS SELECT c3 FROM t3 ORDER BY c4;
SELECT * FROM t1, t2 WHERE c1=(SELECT 123 INTERSECT SELECT c2 FROM t5) AND c1=123;
```

Problem first appeared in the 3.25.0 release on 2018-09-15 and seems to have been caused by the new use of transitive properties for constant propagation - the optimization identified as "3c" in the change log