2021-07-13

15:30 Remove two incorrect assert() statements from the logic used to derive column names and types from subqueries. This allows the SQL associated with CVE-2020-13871 (ticket ~~[c8d3b9f0a750a529]~~) to be tested. (**Closed-Leaf** check-in: d2e67220 user: dan tags: branch-3.28a)

2020-06-08

12:49 When an Expr object is changed and that Expr is referenced by an AggInfo, then also update the AggInfo. Also, persist all AggInfo objects until the Parse object is destroyed. This is a new fix for ticket ~~[c8d3b9f0a750a529]~~. (check-in: 44a58d6c user: drh tags: branch-3.32)

11:34 When an Expr object is changed and that Expr is referenced by an AggInfo, then also update the AggInfo. Also, persist all AggInfo objects until the Parse object is destroyed. This is a new fix for ticket ~~[c8d3b9f0a750a529]~~ that avoids the follow-on problems identified by tickets ~~[8099cf62f597d7e7]~~, ~~[4f6f353b684fc708]~~, ~~[e5504e987e419fb0]~~, and ~~[f7d8980850f361402]~~. (check-in: 6e6b3729 user: drh tags: trunk)

2020-06-07

17:33 Alternative fix to ticket ~~[c8d3b9f0a750a529]~~: Prior to deleting or modifying an Expr not that is referenced by an AggInfo, modify the AggInfo to get its own copy of the original Expr. (check-in: 7682d8a7 user: drh tags: persist-agginfo)

2020-06-05

15:56 Do parse-tree transformations required for window functions prior to running aggregate function analysis. Fix for ticket ~~[c8d3b9f0a750a529]~~. (check-in: 79eff1d0 user: drh tags: branch-3.32-early-winfunc-rewrite)

15:26 • Fixed ticket ~~[c8d3b9f0]~~: *Use after free in resetAccumulator.* plus 5 other changes (artifact: a22f5809 user: drh)

15:26 Do parse-tree transformations required for window functions prior to running aggregate function analysis. Fix for ticket ~~[c8d3b9f0a750a529]~~. (check-in: 0b42a227 user: drh tags: early-winfunc-rewrite-dev)

01:52 • New ticket ~~[c8d3b9f0]~~ *Use after free in resetAccumulator.*. (artifact: cd708fa8 user: yongheng)

Ticket Hash:	c8d3b9f0a750a529ec2f991aa9c8f0d68699f263		
Title:	Use after free in resetAccumulator.		
Status:	Fixed	Type:	Code_Defect
Severity:	Important	Priority:	Low
Subsystem:	Unknown	Resolution:	Fixed
Last Modified:	2020-06-05 15:26:18		
Version Found In:			

User Comments:

yongheng added on 2020-06-05 01:52:37:

```
Release version is affected.

POC:
---
CREATE TABLE a(b);
SELECT(SELECT b FROM a GROUP BY b HAVING(NULL AND b IN((SELECT COUNT() OVER(ORDER BY b) = lead(b) OVER(ORDER BY 3.100000 * SUM(DISTINCT CASE WHEN b LIKE 'SM PACK'
THEN b * b ELSE 0 END) / b))))) FROM a EXCEPT SELECT b FROM a ORDER BY b, b, b;
---
```