Login

SQLite / View Ticket

☰Home Timeline Files Forum

Check-ins History Plaintext

2020-05-23

20:03 • Fixed ticket ~~[23439ea5]~~: *Stack overflow in sqlite3_str_vappendf, caused by int overflow* plus 7 other changes (artifact: 126aa8d4 user: drh)

19:58 ○ Limit the "precision" of floating-point to text conversions in the printf() function to 100,000,000. Fix for ticket ~~[23439ea582241138]~~. (check-in: d08d3405 user: drh tags: trunk)

17:52 • New ticket ~~[23439ea5]~~ *Stack overflow in sqlite3_str_vappendf, caused by int overflow*. (artifact: e6eaff95 user: yongheng)

Ticket Hash:	23439ea5822411389c8edac234c08f2cc27ef3e9		
Title:	Stack overflow in sqlite3_str_vappendf, caused by int overflow		
Status:	Fixed	Type:	Code_Defect
Severity:	Important	Priority:	Low
Subsystem:	Utilities	Resolution:	Fixed
Last Modified:	2020-05-23 20:03:59		
Version Found In:			

User Comments:

yongheng added on 2020-05-23 17:52:02:

```
Affected latest release version.

POC:
---
CREATE TABLE a(b DOUBLE CHECK( NOT CASE WHEN printf(b, b) THEN 0 END) UNIQUE ON CONFLICT REPLACE);
CREATE TRIGGER c INSERT ON a BEGIN INSERT INTO a SELECT group_concat(b, 2147483647) FROM a;END;
INSERT INTO a(b, b, b) VALUES(NULL, 9, 3);
UPDATE a SET b = 0;
INSERT INTO a VALUES('GERMANY''s%'), ('Y'), ('Brand#23')
---
```

drh added on 2020-05-23 20:03:59:

Simplified test case:

```
SELECT printf('%.*g',2147483647,0.01);
```

Affects all versions of SQLite since printf() was introduced in version 3.8.3 (2014-02-03).