
Subject: underflow in bool Sql::fetch()

Posted by [grc3H0219](#) on Sat, 26 Jul 2008 17:15:14 GMT

[View Forum Message](#) <> [Reply to Message](#)

Hello:

I have been Ultimate++ with sqlite3 for about 4 months and have found Ultimate++ very easy to use. I am using TheIDE 2008.2 beta 2008-03-24 9:41, Mingw and Windows XP Professional SP2. I have run into a few very minor problems.

The first problem is with bool Sql::fetch() and was mentioned in message #14083.

(<http://www.ultimatepp.org/forum/index.php?t=msg&goto=14091&>)

The patch corrected the integer overflow of the positive values.

I am seeing integer overflow(underflow) in negative values such that when t is small compared to starttime and traceslow,

- session.traceslow - cn->starttime

is smaller than -(INT_MAX) and is converted to a large positive number instead the small negative value that it is. This results in the output of all SQL statements to the BugLog file. In bool Sql::Fetch(),

When I convert the

bool Sql::fetch() code: if(t - session.traceslow - cn->starttime > 0)

to: if((float)t - (float)session.traceslow - (float)cn->starttime > 0)

or to: if((signed long long)t - (signed long long)session.traceslow - (signed long long)cn->starttime > 0)

the correct number is generated. The following values are typical numbers for t, starttime and traceslow on my system:

t: 2076696 starttime: 2147483647 traceslow: 536870911

In SqlSession::SqlSession(),

traceslow = INT_MAX / 4; So, if t is less than INT_MAX / 4, there will be an integer overflow error.

dw

Subject: Re: underflow in bool Sql::fetch()

Posted by [mirek](#) on Sat, 26 Jul 2008 18:11:33 GMT

[View Forum Message](#) <> [Reply to Message](#)

grc3H0219 wrote on Sat, 26 July 2008 13:15Hello:

I have been Ultimate++ with sqlite3 for about 4 months and have found Ultimate++ very easy to use. I am using TheIDE 2008.2

beta 2008-03-24 9:41, Mingw and Windows XP Professional SP2. I have run into a few very minor

problems.

The first problem is with `bool Sql::fetch()` and was mentioned in message #14083.

(<http://www.ultimatepp.org/forum/index.php?t=msg&goto=14091&>)

The patch corrected the integer overflow of the positive values.

I am seeing integer overflow (underflow) in negative values such that when `t` is small compared to `starttime` and `traceslow`,

`- session.traceslow - cn->starttime`

is smaller than `-(INT_MAX)` and is converted to a large positive number instead of the small negative value that it is. This results in the output of all SQL statements to the BugLog file. In `bool Sql::Fetch()`,

When I convert the

`bool Sql::fetch()` code: `if(t - session.traceslow - cn->starttime > 0)`

to: `if((float)t - (float)session.traceslow - (float)cn->starttime > 0)`

or to: `if((signed long long)t - (signed long long)session.traceslow - (signed long long)cn->starttime > 0)`

the correct number is generated. The following values are typical numbers for `t`, `starttime` and `traceslow` on my system:

`t: 2076696 starttime: 2147483647 traceslow: 536870911`

In `SqlSession::SqlSession()`,

`traceslow = INT_MAX / 4`; So, if `t` is less than `INT_MAX / 4`, there will be an integer overflow error.

dw

Which U++ version? I was fixing this issue 3 weeks ago, if I remember well..

If it is not a problem confirmed with latest release (2008.1 final), can you check with it?

Mirek

Subject: Re: underflow in `bool Sql::fetch()`

Posted by [grc3H0219](#) on Sat, 26 Jul 2008 21:20:54 GMT

[View Forum Message](#) <> [Reply to Message](#)

I was using `upp-mingw-2008.2beta`. With `upp-mingw-2008.1rc2` this problem has been resolved. Thanks.

dw