# QGIS Application - Bug report #6170
# Heap corruption in PAL

2012-08-08 08:30 AM - Matthias Kuhn

| | | | |
|---|---|---|---|
| **Status:** | Closed | | |
| **Priority:** | Normal | | |
| **Assignee:** | Matthias Kuhn | | |
| **Category:** | | | |
| **Affected QGIS version:** | master | **Regression?:** | No |
| **Operating System:** | | **Easy fix?:** | No |
| **Pull Request or Patch supplied:** | No | **Resolution:** | |
| **Crashes QGIS or corrupts data:** | No | **Copied to github as #:** | 15488 |

**Description**

My debugger (VS2008) was complaining about a heap corruption. After some investigation I could locate the following:

costcalculator.h:
double dist[8];

costcalculator.cpp, line 275 (in void PolygonCostCalculator::updatePoint( PointSet *pset )):

int i = ( int )( beta / a45 );

[...]
dist[i] = d;

Guess what happens if i == 8
Probably nothing unless you happen to have something important after the dist array.

Now you might wonder, how comes, that i is 8. I've no idea why, but I guess that following pure math it shouldn't.

Back to line 275
i = beta / a45

In my case beta = 6.2831853071795862 and a45 = 0.78539816339744828
My windows calc shows me as the result 7.9999999999999999490704182105935 which should be rounded to 7. But my debugger shows me 8.

I don't whose fault it is that windows calculator gives another result than dividing two doubles does, but there seems to be something wrong.

## Associated revisions

**Revision 928da6e3 - 2012-08-08 07:04 PM - Jürgen Fischer**

fix #6170

## History

**#1 - 2012-08-08 10:04 AM - Jürgen Fischer**

*- Status changed from Open to Closed*

Fixed in changeset commit:"928da6e3bb435da0112bb373096871597012e212".