U++ - Bug #497
Ide/Browser: ParseItemNatural function with empty name

07/28/2013 06:39 PM - Sender Ghost

Status:	Approved		**Start date:**	07/28/2013
Priority:	Normal		**Due date:**	
Assignee:	Sender Ghost		**% Done:**	0%
Category:	IDE		**Estimated time:**	0.00 hour
Target version:			**Spent time:**	0.00 hour

Description

The following excerpt from C/C++ source code leads to "Out of memory" panic message inside of <u>ParseItemNatural</u> function:

    a :2:

But also applicable for //**$** comment:

    //$Id: Description 1234-12-12 12:34:56Z nickname $

History

#1 - 07/28/2013 06:48 PM - Sender Ghost

- File 497a_uppsrc.diff added

- File 497b_uppsrc.diff added

- Status changed from New to Patch ready

I think, the cause with empty name might be related to C++ <u>parser</u>.

But anyway, the **ParseItemNatural** function is not guarded against empty name and some combination of ':' character (when <u>n = 0</u> and Vector <u>grows</u> to memory limit inside of <u>unlimited</u> while loop). The simple fix is to check the length of the **name** variable, but also possible to reorganize <u>creation</u> of new Vector item to the moment, when final n value is known (e.g. near <u>s += n</u>, else ++s in case of n == 0).

Therefore, I created two different patches for **ParseItemNatural** function, which might be incomplete.

#2 - 07/29/2013 06:51 PM - Miroslav Fidler

- Status changed from Patch ready to Approved

- Assignee changed from Miroslav Fidler to Sender Ghost

thanks!

#3 - 07/30/2013 09:06 AM - Sender Ghost

- File 497a_uppsrc2.diff added

I created additional patch (for variant a), which uses **m.natural** value length to show some text for Navigator bar, instead of just empty string.

This returns ability to show **INITBLOCK**, **CONSOLE_APP_MAIN**, **GUI_APP_MAIN** kind of defines for Navigator bar.

#4 - 07/30/2013 09:06 AM - Sender Ghost

- Status changed from Approved to Patch ready

- Assignee changed from Sender Ghost to Miroslav Fidler

#5 - 07/30/2013 06:48 PM - Sender Ghost

- Status changed from Patch ready to Approved

- Assignee changed from Miroslav Fidler to Sender Ghost

r6218

Files

497a_uppsrc.diff	887 Bytes	07/28/2013		Sender Ghost
497b_uppsrc.diff	1.14 KB	07/28/2013		Sender Ghost
497a_uppsrc2.diff	590 Bytes	07/30/2013		Sender Ghost

#5 - 07/30/2013 06:48 PM - Sender Ghost

- Status changed from Patch ready to Approved

- Assignee changed from Miroslav Fidler to Sender Ghost