Subject: Infinite loop in Parser
Posted by Didier on Wed, 26 Apr 2017 21:32:54 GMT
View Forum Message <> Reply to Message

Hello Mirek,

I have a very annoying problem with the source indexing parser : it goes into an infinite loop at: uppsrc/CppBase/Parser.cpp

The bug has been around for some time now and it fails to parse the Boost header files (boost 1.63.0 to be precise)
It stays stuck at lines 105->114

File Attachments

1) ParserInifiteLoop.png, downloaded 809 times

```
1: s
0x7fffc3d671dd "()( typename impl::expr_param e , typename impl::state_param , typename impl::data_param ) c
```

Locals

```
w     = 0x7fffc3d671dd "()( typename impl::expr_param e , typename impl::state_param , typename impl::data_
c     = 40 '('
res   = {...}
wasid = true
```

Args

```
s     = 0x7fffc3d671dd "()( typename impl::expr_param e , typename impl::state_param , typename impl::data_
pname = 0x7ffffffbd7c0 "e"
qname = 0x7fffc2acde68 ""
name  = <?pointer_value>
oper  = false
```

```
103         }
104         bool wasid = false;
105         while(*s) {
106                 const char *w = bew(qname, s);
107                 byte c = *s;
108                 if(w && !iscid(*w)) {
109                         if(iscid(*res.Last()))
110                                 res.Cat(' ');
111                         res.Cat(name);
112                         s = w;
113                         wasid = true;
114                 }
115                 else
116                 if(iscid(c)) {
117                         const char *b = s++;
118                         while(iscid(*s)) s++;
119                         String q(b, s);
120                         if(q != s_virtual && q != s_inline && q != s_static && !InScList(q, pname)) {
121                                 if(iscid(*res.Last()))
122                                         res.Cat(' ');
123                                 res.Cat(q);
124                         }
125                         else
126                                 while((byte)*s <= ' ' && *s) s++;
127                         wasid = true;
128                 }
```

```
(gdb) next
```