Subject: [FIXED] String::Replace(empty string,) => Out of memory!
Posted by omari on Fri, 02 May 2014 14:16:47 GMT
View Forum Message <> Reply to Message

Hi,

a call to String::Replace(f, r) crash if f.GetCount is equal to 0, with message:

Out of memory!
Request size : 905969755 B
U++ allocated memory: 442520 KB

I found that is because Replace use t_find (StringFind.hpp line 30):

template <int step> // Template parameter to be a constant
int t_find(const char *ptr, int slen, const char *p, int len, int from)

and t_find returns 0 if slen is equal to 0.

```
 else
 if(len == 1) {
  char p0 = p[0];
  while(s <= e) {
   if(*s == p0)
    return (int)(s - ptr);
   s += step;
  }
 }
 else
  return 0;   <---- (line 87)
```

if t_find return -1 instead of 0, it resolve the issu.

Regards
omari.

Subject: Re: [BUG] String::Replace(empty string,) => Out of memory!
Posted by mirek on Fri, 02 May 2014 16:27:18 GMT
View Forum Message <> Reply to Message

Well, this is an interesting issue. While obviously it should not crash, I somehow doubt that returning -1 is correct here.

More specifically, I believe that

String h("xxx");
h.Find("");

should return 0, because there IS empty substring at position 0 after all. In any case, such behaviour is consistent with e.g. STL (and I suspect all other libraries).

```
CONSOLE_APP_MAIN {
 std::string s = "xxxxxx";
 DDUMP(s.find(""));
}
```

Means, specifying empty string as string to be replaced is sort of illegal. Anyway, I have added a check to Replace. Thanks for pointing that out...

Mirek

Subject: Re: [BUG] String::Replace(empty string,) => Out of memory!
Posted by omari on Fri, 02 May 2014 17:03:01 GMT
View Forum Message <> Reply to Message

thanks Mirek, problem solved.

i am agree any string has the empty substring, but how many times?
 - 1 at position 0
 - or 1 at position 0 and 1 at the end
 - or infinity?

if there is more than one, i think t_find can returns (from).

what do you think?

Subject: Re: [BUG] String::Replace(empty string,) => Out of memory!
Posted by mirek on Sat, 03 May 2014 13:52:19 GMT
View Forum Message <> Reply to Message

omari wrote on Fri, 02 May 2014 19:03thanks Mirek, problem solved.

i am agree any string has the empty substring, but how many times?

- 1 at position 0
- or 1 at position 0 and 1 at the end
- or infinity?

if there is more than one, i think t_find can returns (from).

what do you think?

Right! Sorry, somehow I forgot to account for "from".

Mirek
