Subject: Re: theide with libclang
Posted by jjacksonRIAB on Tue, 20 Sep 2022 19:32:31 GMT
View Forum Message <> Reply to Message

OK so with address sanitizer and USEMALLOC enabled, I'm getting a bunch of reported heap overflows all on memcmp.

lib/clang Signature.cpp line 171, for example:

if(memcmp(s, " = {", 4) == 0)

what happens if s is shorter than the sequence it's being compared against? Does it overrun?