

[New issue](#)[Jump to bottom](#)

# Multiple Heap Buffer Overflows in PicoC at Various Locations

## #37

Open Halcy0nic opened this issue on Oct 25 · 0 comments

Halcy0nic commented on Oct 25

Hi,

I was running my fuzz tests in the background and discovered multiple heap buffer overflows in PicoC Version 3.2.2 at various locations. After triaging all of the crashes, I can verify that there are 10 separate and unique heap buffer overflows at the following locations:

- **StdioBasePrintf** in `cstdlib/stdio.c` when called from `ExpressionParseFunctionCall` in `expression.c`
- **LexGetStringConstant** in `lex.c` when called from `LexScanGetToken` in `lex.c`
- **ExpressionCoerceUnsignedInteger** in `expression.c` when called from `ExpressionParseFunctionCall` in `expression.c`
- **ExpressionCoerceInteger** in `expression.c` when called from `ExpressionInfixOperator` in `expression.c`
- **ExpressionAssign** in `expression.c` when called from `ExpressionParseMacroCall` in `expression.c`
- **StringStrcat** in `cstdlib/string.c` when called from `ExpressionParseFunctionCall` in `expression.c`
- **StringStrncpy** in `cstdlib/string.c` when called from `ExpressionParseFunctionCall` in `expression.c`
- **ExpressionCoerceFP** in `expression.c` when called from `ExpressionParseFunctionCall` in `expression.c`
- **StdioOutPutc** in `cstdlib/stdio.c` when called from `ExpressionParseFunctionCall` in `expression.c`
- **LexSkipComment** in `lex.c` when called from `LexScanGetToken` in `lex.c`

## Reproduction and Details

For each of the heap buffer overflows I have attached a reproduction file and the full output from [ASAN \(address sanitizer\)](#). The easiest way to reproduce each overflow would be to run the relevant file through the interpreter:

```
picoc -s [reproduction_filename.c]
```

# StdioBasePrintf in cstdlib/stdio.c when called from ExpressionParseFunctionCall in expression.c.

File for Reprotuction: [cstdlib\\_stdio\\_heap\\_overflow.c.zip](#)

```
=====
==912065==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60300000563b at pc
0x562a94fe1ae8 bp 0x7ffc0f423270 sp 0x7ffc0f423268
READ of size 1 at 0x60300000563b thread T0
    #0 0x562a94fe1ae7 in StdioBasePrintf cstdlib/stdio.c:249
    #1 0x562a94fe4e9f in StdioPrintf cstdlib/stdio.c:682
    #2 0x562a94fd2edd in ExpressionParseFunctionCall
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1909
    #3 0x562a94fd037c in ExpressionParse
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1607
    #4 0x562a94fc46a0 in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:646
    #5 0x562a94fc3b07 in ParseBlock /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:558
    #6 0x562a94fc474b in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:651
    #7 0x562a94fc0028 in ParseStatementMaybeRun
/home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:54
    #8 0x562a94fc49db in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:681
    #9 0x562a94fc6380 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:897
    #10 0x562a94fded0e in PicocPlatformScanFile platform/platform_unix.c:129
    #11 0x562a94fb5213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
    #12 0x7fb5e3fe57fc in __libc_start_main ../csu/libc-start.c:332
    #13 0x562a94fb4d49 in _start (/home/kali/projects/fuzzing/fuzz_targets/picoc/picoc+0x16d49)

0x60300000563b is located 0 bytes to the right of 27-byte region [0x603000005620,0x60300000563b)
allocated by thread T0 here:
    #0 0x7fb5e43e0987 in __interceptor_malloc
../../src/libsanitizer/asan/asan_malloc_linux.cpp:154
    #1 0x562a94fd3b80 in HeapAllocMem /home/kali/projects/fuzzing/fuzz_targets/picoc/heap.c:127
    #2 0x562a94fb624a in TableSetIdentifier
/home/kali/projects/fuzzing/fuzz_targets/picoc/table.c:162
    #3 0x562a94fb645b in TableStrRegister2
/home/kali/projects/fuzzing/fuzz_targets/picoc/table.c:179
    #4 0x562a94fb9965 in LexGetStringConstant
/home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:390
    #5 0x562a94fbac4f in LexScanGetToken /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:502
    #6 0x562a94fbbfc6 in LexTokenize /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:642
    #7 0x562a94fbc527 in LexAnalyse /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:704
    #8 0x562a94fc61b7 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:874
    #9 0x562a94fded0e in PicocPlatformScanFile platform/platform_unix.c:129
    #10 0x562a94fb5213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
    #11 0x7fb5e3fe57fc in __libc_start_main ../csu/libc-start.c:332

SUMMARY: AddressSanitizer: heap-buffer-overflow cstdlib/stdio.c:249 in StdioBasePrintf
Shadow bytes around the buggy address:
 0x0c067fff8a70: fd fd fd fa fa fa 00 00 00 00 fa fa fd fd fd fa
 0x0c067fff8a80: fa fa fd fd fd fa fa fa 00 00 00 00 fa fa fd fd
 0x0c067fff8a90: fd fa fa fa 00 00 00 00 fa fa fd fd fd fa fa fa
 0x0c067fff8aa0: 00 00 00 00 fa fa fd fd fd fa fa fa 00 00 00 00
 0x0c067fff8ab0: fa fa fd fd fd fa fa fa 00 00 00 02 fa fa 00 00
=>0x0c067fff8ac0: 00 02 fa fa 00 00 00[03]fa fa 00 00 00 03 fa fa
```

```
0x0c067fff8ad0: 00 00 00 07 fa fa 00 00 00 02 fa fa 00 00 00 02
0x0c067fff8ae0: fa fa 00 00 00 05 fa fa 00 00 00 02 fa fa 00 00
0x0c067fff8af0: 00 fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c067fff8b00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c067fff8b10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
```

```
Addressable:          00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:    fa
Freed heap region:    fd
Stack left redzone:   f1
Stack mid redzone:    f2
Stack right redzone:  f3
Stack after return:   f5
Stack use after scope: f8
Global redzone:       f9
Global init order:    f6
Poisoned by user:     f7
Container overflow:    fc
Array cookie:          ac
Intra object redzone: bb
ASan internal:         fe
Left alloca redzone:  ca
Right alloca redzone: cb
Shadow gap:           cc
```

```
==912065==ABORTING
```

## LexGetStringConstant in lex.c when called from LexScanGetToken in lex.c.

---

File for Reproduction:

[LexGetStringConstant\\_lex\\_heap\\_overflow.c.zip](#)

```
=====
==912099==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60c0000000b5 at pc
0x558299178802 bp 0x7ffcde91cc50 sp 0x7ffcde91cc48
READ of size 1 at 0x60c0000000b5 thread T0
#0 0x558299178801 in LexGetStringConstant
/home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:361
#1 0x558299179c4f in LexScanGetToken /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:502
#2 0x55829917afc6 in LexTokenize /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:642
#3 0x55829917b527 in LexAnalyse /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:704
#4 0x5582991851b7 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:874
#5 0x55829919dd0e in PicocPlatformScanFile platform/platform_unix.c:129
#6 0x558299174213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
#7 0x7fee5afb97fc in __libc_start_main ../csu/libc-start.c:332
#8 0x558299173d49 in _start (/home/kali/projects/fuzzing/fuzz_targets/picoc/picoc+0x16d49)

0x60c0000000b5 is located 0 bytes to the right of 117-byte region [0x60c000000040,0x60c0000000b5)
allocated by thread T0 here:
```

```

#0 0x7fee5b3b47cf in __interceptor_malloc
.././././././src/libsanitizer/asan/asan_malloc_linux.cpp:145
#1 0x55829919d8a7 in PlatformReadFile platform/platform_unix.c:94
#2 0x55829919dbfc in PicocPlatformScanFile platform/platform_unix.c:121
#3 0x558299174213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
#4 0x7fee5afb97fc in __libc_start_main ../csu/libc-start.c:332

```

SUMMARY: AddressSanitizer: heap-buffer-overflow

/home/kali/projects/fuzzing/fuzz\_targets/picoc/lex.c:361 in LexGetStringConstant

Shadow bytes around the buggy address:

```

0x0c187fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c187fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c187fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c187fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c187fff8000: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00
=>0x0c187fff8010: 00 00 00 00 00 00 00[05]fa fa fa fa fa fa fa fa
0x0c187fff8020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 fa
0x0c187fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c187fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c187fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c187fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

```

Shadow byte legend (one shadow byte represents 8 application bytes):

```

Addressable:           00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:      fa
Freed heap region:      fd
Stack left redzone:     f1
Stack mid redzone:      f2
Stack right redzone:    f3
Stack after return:     f5
Stack use after scope:  f8
Global redzone:         f9
Global init order:      f6
Poisoned by user:       f7
Container overflow:      fc
Array cookie:           ac
Intra object redzone:   bb
ASan internal:          fe
Left alloca redzone:    ca
Right alloca redzone:   cb
Shadow gap:             cc

```

==912099==ABORTING

## ExpressionCoerceUnsignedInteger in expression.c when called from ExpressionParseFunctionCall in expression.c.

File for Reprotuction:

[ExpressionCoerceUnsignedInteger\\_heap\\_overflow.c.zip](#)

=====

==912164==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60700000230 at pc 0x563f0e1b0f72 bp 0x7ffc1ad03030 sp 0x7ffc1ad03028

READ of size 4 at 0x60700000230 thread T0

#0 0x563f0e1b0f71 in ExpressionCoerceUnsignedInteger  
/home/kali/projects/fuzzing/fuzz\_targets/picoc/expression.c:270  
#1 0x563f0e1cb451 in StdioBasePrintf cstdlib/stdio.c:379  
#2 0x563f0e1cee9f in StdioPrintf cstdlib/stdio.c:682  
#3 0x563f0e1bcedd in ExpressionParseFunctionCall  
/home/kali/projects/fuzzing/fuzz\_targets/picoc/expression.c:1909  
#4 0x563f0e1ba37c in ExpressionParse  
/home/kali/projects/fuzzing/fuzz\_targets/picoc/expression.c:1607  
#5 0x563f0e1ae6a0 in ParseStatement /home/kali/projects/fuzzing/fuzz\_targets/picoc/parse.c:646  
#6 0x563f0e1ad6c1 in ParseFor /home/kali/projects/fuzzing/fuzz\_targets/picoc/parse.c:524  
#7 0x563f0e1aee02 in ParseStatement /home/kali/projects/fuzzing/fuzz\_targets/picoc/parse.c:715  
#8 0x563f0e1b0380 in PicocParse /home/kali/projects/fuzzing/fuzz\_targets/picoc/parse.c:897  
#9 0x563f0e1c8d0e in PicocPlatformScanFile platform/platform\_unix.c:129  
#10 0x563f0e19f213 in main /home/kali/projects/fuzzing/fuzz\_targets/picoc/picoc.c:62  
#11 0x7f1dbc2477fc in \_\_libc\_start\_main ../csu/libc-start.c:332  
#12 0x563f0e19ed49 in \_start (/home/kali/projects/fuzzing/fuzz\_targets/picoc/picoc+0x16d49)

0x60700000230 is located 0 bytes to the right of 80-byte region [0x6070000001e0,0x607000000230) allocated by thread T0 here:

#0 0x7f1dbc642987 in \_\_interceptor\_calloc  
.././././././src/libsanitizer/asan/asan\_malloc\_linux.cpp:154  
#1 0x563f0e1bdb80 in HeapAllocMem /home/kali/projects/fuzzing/fuzz\_targets/picoc/heap.c:127  
#2 0x563f0e1c23a9 in VariableAlloc  
/home/kali/projects/fuzzing/fuzz\_targets/picoc/variable.c:77  
#3 0x563f0e1c2429 in VariableAllocValueAndData  
/home/kali/projects/fuzzing/fuzz\_targets/picoc/variable.c:97  
#4 0x563f0e1c2701 in VariableAllocValueFromType  
/home/kali/projects/fuzzing/fuzz\_targets/picoc/variable.c:119  
#5 0x563f0e1c3aa7 in VariableDefine  
/home/kali/projects/fuzzing/fuzz\_targets/picoc/variable.c:303  
#6 0x563f0e1c46aa in VariableDefineButIgnoreIdentical  
/home/kali/projects/fuzzing/fuzz\_targets/picoc/variable.c:383  
#7 0x563f0e1ac540 in ParseDeclaration  
/home/kali/projects/fuzzing/fuzz\_targets/picoc/parse.c:366  
#8 0x563f0e1aef6e in ParseStatement /home/kali/projects/fuzzing/fuzz\_targets/picoc/parse.c:738  
#9 0x563f0e1b0380 in PicocParse /home/kali/projects/fuzzing/fuzz\_targets/picoc/parse.c:897  
#10 0x563f0e1c8d0e in PicocPlatformScanFile platform/platform\_unix.c:129  
#11 0x563f0e19f213 in main /home/kali/projects/fuzzing/fuzz\_targets/picoc/picoc.c:62  
#12 0x7f1dbc2477fc in \_\_libc\_start\_main ../csu/libc-start.c:332

SUMMARY: AddressSanitizer: heap-buffer-overflow

/home/kali/projects/fuzzing/fuzz\_targets/picoc/expression.c:270 in ExpressionCoerceUnsignedInteger  
Shadow bytes around the buggy address:

0x0c0e7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x0c0e7fff8000: fa fa fa fa fd fd fd fd fd fd fd fd fd fa fa  
0x0c0e7fff8010: fa fa fd fd fd fd fd fd fd fd fd fa fa fa fa  
0x0c0e7fff8020: 00 00 00 00 00 00 00 00 05 fa fa fa fa 00 00  
0x0c0e7fff8030: 00 00 00 00 00 00 00 00 fa fa fa fa 00 00 00  
=>0x0c0e7fff8040: 00 00 00 00 00 00 [fa]fa fa fa fa fa fa fa fa  
0x0c0e7fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0c0e7fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

```

0x0c0e7fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0e7fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0e7fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable:          00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:    fa
Freed heap region:    fd
Stack left redzone:    f1
Stack mid redzone:     f2
Stack right redzone:   f3
Stack after return:    f5
Stack use after scope: f8
Global redzone:        f9
Global init order:     f6
Poisoned by user:      f7
Container overflow:    fc
Array cookie:          ac
Intra object redzone:  bb
ASan internal:         fe
Left alloca redzone:   ca
Right alloca redzone:  cb
Shadow gap:            cc
==912164==ABORTING

```

## ExpressionAssign in expression.c when called from ExpressionParseMacroCall in expression.c.

---

File for Reprotuction:

[ExpressionAssign\\_heap\\_overflow.c.zip](#)

```

=====
==912198==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000005608 at pc
0x563053b280cb bp 0x7ffe0502f540 sp 0x7ffe0502f538
READ of size 8 at 0x603000005608 thread T0
#0 0x563053b280ca in ExpressionAssign
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:516
#1 0x563053b309ba in ExpressionParseMacroCall
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1781
#2 0x563053b30d30 in ExpressionParseFunctionCall
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1805
#3 0x563053b2f37c in ExpressionParse
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1607
#4 0x563053b31253 in ExpressionParseFunctionCall
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1834
#5 0x563053b2f37c in ExpressionParse
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1607
#6 0x563053b236a0 in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:646
#7 0x563053b25380 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:897
#8 0x563053b3dd0e in PicocPlatformScanFile platform/platform_unix.c:129

```

```
#9 0x563053b14213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
#10 0x7f94cf72f7fc in __libc_start_main ../csu/libc-start.c:332
#11 0x563053b13d49 in _start (/home/kali/projects/fuzzing/fuzz_targets/picoc/picoc+0x16d49)
```

0x60300000560f is located 0 bytes to the right of 31-byte region [0x6030000055f0,0x60300000560f) allocated by thread T0 here:

```
#0 0x7f94cfb2a987 in __interceptor_calloc
.././././././src/libsanitizer/asan/asan_malloc_linux.cpp:154
#1 0x563053b32b80 in HeapAllocMem /home/kali/projects/fuzzing/fuzz_targets/picoc/heap.c:127
#2 0x563053b1524a in TableSetIdentifier
/home/kali/projects/fuzzing/fuzz_targets/picoc/table.c:162
#3 0x563053b1545b in TableStrRegister2
/home/kali/projects/fuzzing/fuzz_targets/picoc/table.c:179
#4 0x563053b17910 in LexGetWord /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:254
#5 0x563053b199f8 in LexScanGetToken /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:493
#6 0x563053b1afc6 in LexTokenize /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:642
#7 0x563053b1b527 in LexAnalyse /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:704
#8 0x563053b251b7 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:874
#9 0x563053b3dd0e in PicocPlatformScanFile platform/platform_unix.c:129
#10 0x563053b14213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
#11 0x7f94cf72f7fc in __libc_start_main ../csu/libc-start.c:332
```

SUMMARY: AddressSanitizer: heap-buffer-overflow

/home/kali/projects/fuzzing/fuzz\_targets/picoc/expression.c:516 in ExpressionAssign

Shadow bytes around the buggy address:

```
0x0c067fff8a70: fd fd fd fa fa fa 00 00 00 00 fa fa fd fd fd fa
0x0c067fff8a80: fa fa fd fd fd fa fa fa 00 00 00 00 fa fa fd fd
0x0c067fff8a90: fd fa fa fa 00 00 00 00 fa fa fd fd fd fa fa fa
0x0c067fff8aa0: 00 00 00 00 fa fa fd fd fd fa fa fa 00 00 00 00
0x0c067fff8ab0: fa fa fd fd fd fa fa fa 00 00 00 05 fa fa 00 00
=>0x0c067fff8ac0: 00[07]fa fa 00 00 00 02 fa fa 00 00 00 04 fa fa
0x0c067fff8ad0: 00 00 00 05 fa fa 00 00 00 05 fa fa 00 00 00 fa
0x0c067fff8ae0: fa fa 00 00 00 00 fa fa fa fa fa fa fa fa fa fa
0x0c067fff8af0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c067fff8b00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c067fff8b10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

Shadow byte legend (one shadow byte represents 8 application bytes):

```
Addressable:           00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:      fa
Freed heap region:      fd
Stack left redzone:     f1
Stack mid redzone:      f2
Stack right redzone:    f3
Stack after return:     f5
Stack use after scope:  f8
Global redzone:         f9
Global init order:      f6
Poisoned by user:       f7
Container overflow:     fc
Array cookie:           ac
Intra object redzone:   bb
ASan internal:          fe
Left alloca redzone:    ca
Right alloca redzone:   cb
```

```
Shadow gap:                cc
==912198==ABORTING
```

## StringStrcat in cstdlib/string.c L40 when called from ExpressionParseFunctionCall in expression.c.

---

File for Reprotuction:

[StringStrcat\\_heap\\_overflow.c.zip](#)

```
=====
==912341==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x606000000832 at pc
0x7f93cb901590 bp 0x7ffc7cfa1530 sp 0x7ffc7cfa0ce0
WRITE of size 26 at 0x606000000832 thread T0
    #0 0x7f93cb90158f in __interceptor_strcat
    ../../../../src/libsanitizer/asan/asan_interceptors.cpp:392
    #1 0x561b032f2412 in StringStrcat cstdlib/string.c:40
    #2 0x561b032dbedd in ExpressionParseFunctionCall
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1909
    #3 0x561b032d937c in ExpressionParse
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1607
    #4 0x561b032cd6a0 in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:646
    #5 0x561b032cf380 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:897
    #6 0x561b032e7d0e in PicocPlatformScanFile platform/platform_unix.c:129
    #7 0x561b032be213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
    #8 0x7f93cb57a7fc in __libc_start_main ../csu/libc-start.c:332
    #9 0x561b032bdd49 in _start (/home/kali/projects/fuzzing/fuzz_targets/picoc/picoc+0x16d49)

0x606000000832 is located 0 bytes to the right of 50-byte region [0x606000000800,0x606000000832)
allocated by thread T0 here:
    #0 0x7f93cb975987 in __interceptor_calloc
    ../../../../src/libsanitizer/asan/asan_malloc_linux.cpp:154
    #1 0x561b032dcb80 in HeapAllocMem /home/kali/projects/fuzzing/fuzz_targets/picoc/heap.c:127
    #2 0x561b032e13a9 in VariableAlloc
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:77
    #3 0x561b032e1429 in VariableAllocValueAndData
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:97
    #4 0x561b032e1701 in VariableAllocValueFromType
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:119
    #5 0x561b032e2aa7 in VariableDefine
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:303
    #6 0x561b032e36aa in VariableDefineButIgnoreIdentical
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:383
    #7 0x561b032cb540 in ParseDeclaration
/home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:366
    #8 0x561b032cdf6e in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:738
    #9 0x561b032cf380 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:897
    #10 0x561b032e7d0e in PicocPlatformScanFile platform/platform_unix.c:129
    #11 0x561b032be213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
    #12 0x7f93cb57a7fc in __libc_start_main ../csu/libc-start.c:332
```



```

SUMMARY: AddressSanitizer: heap-buffer-overflow
../../../../src/libsanitizer/asan/asan_interceptors.cpp:392 in __interceptor_strcat
Shadow bytes around the buggy address:
 0x0c0c7fff80b0: fd fd fd fa fa fa fa fd fd fd fd fd fd fd fa
 0x0c0c7fff80c0: fa fa fa fa fd fd fd fd fd fd fd fa fa fa fa
 0x0c0c7fff80d0: 00 00 00 00 00 00 06 fa fa fa fa fa 00 00 00 00
 0x0c0c7fff80e0: 00 00 00 00 fa fa fa fa 00 00 00 00 00 00 02 fa
 0x0c0c7fff80f0: fa fa fa fa 00 00 00 00 00 00 00 00 fa fa fa fa
=>0x0c0c7fff8100: 00 00 00 00 00 00[02]fa fa fa fa fa fa fa fa
 0x0c0c7fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0c7fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0c7fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0c7fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0c7fff8150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable:          00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:    fa
Freed heap region:    fd
Stack left redzone:   f1
Stack mid redzone:    f2
Stack right redzone:  f3
Stack after return:   f5
Stack use after scope: f8
Global redzone:       f9
Global init order:    f6
Poisoned by user:     f7
Container overflow:    fc
Array cookie:          ac
Intra object redzone: bb
ASan internal:         fe
Left alloca redzone:  ca
Right alloca redzone: cb
Shadow gap:           cc
==912341==ABORTING

```

## StringStrncpy in cstdlib/string.c L19 when called from ExpressionParseFunctionCall in expression.c.

File for Reprotuction:

[StringStrncpy\\_heap\\_overflow.c.zip](#)

```

=====
==912388==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6060000007d2 at pc
0x7f4683a4db45 bp 0x7fff7dde02e0 sp 0x7fff7dddfa90
WRITE of size 22 at 0x6060000007d2 thread T0
#0 0x7f4683a4db44 in __interceptor_strncpy
../../../../src/libsanitizer/asan/asan_interceptors.cpp:485
#1 0x55a9a96daf48 in StringStrncpy cstdlib/string.c:19
#2 0x55a9a96c4edd in ExpressionParseFunctionCall

```

```
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1909
#3 0x55a9a96c237c in ExpressionParse
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1607
#4 0x55a9a96b66a0 in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:646
#5 0x55a9a96b8380 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:897
#6 0x55a9a96d0d0e in PicocPlatformScanFile platform/platform_unix.c:129
#7 0x55a9a96a7213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
#8 0x7f46836a77fc in __libc_start_main ../csu/libc-start.c:332
#9 0x55a9a96a6d49 in _start (/home/kali/projects/fuzzing/fuzz_targets/picoc/picoc+0x16d49)
```

0x606000007d2 is located 0 bytes to the right of 50-byte region [0x606000007a0,0x606000007d2) allocated by thread T0 here:

```
#0 0x7f4683aa2987 in __interceptor_calloc
../../../../../src/libsanitizer/asan/asan_malloc_linux.cpp:154
#1 0x55a9a96c5b80 in HeapAllocMem /home/kali/projects/fuzzing/fuzz_targets/picoc/heap.c:127
#2 0x55a9a96ca3a9 in VariableAlloc
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:77
#3 0x55a9a96ca429 in VariableAllocValueAndData
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:97
#4 0x55a9a96ca701 in VariableAllocValueFromType
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:119
#5 0x55a9a96cbaa7 in VariableDefine
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:303
#6 0x55a9a96cc6aa in VariableDefineButIgnoreIdentical
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:383
#7 0x55a9a96b4540 in ParseDeclaration
/home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:366
#8 0x55a9a96b6f6e in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:738
#9 0x55a9a96b8380 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:897
#10 0x55a9a96d0d0e in PicocPlatformScanFile platform/platform_unix.c:129
#11 0x55a9a96a7213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
#12 0x7f46836a77fc in __libc_start_main ../csu/libc-start.c:332
```

SUMMARY: AddressSanitizer: heap-buffer-overflow

../../../../../src/libsanitizer/asan/asan\_interceptors.cpp:485 in \_\_interceptor\_strncpy

Shadow bytes around the buggy address:

```
0x0c0c7fff80a0: fd fd fd fd fd fd fa fa fa fa fd fd fd fd
0x0c0c7fff80b0: fd fd fd fa fa fa fa fa fd fd fd fd fd fd fa
0x0c0c7fff80c0: fa fa fa fa fd fd fd fd fd fd fa fa fa fa fa
0x0c0c7fff80d0: 00 00 00 00 00 00 06 fa fa fa fa 00 00 00 00
0x0c0c7fff80e0: 00 00 00 00 fa fa fa fa 00 00 00 00 00 00 00
=>0x0c0c7fff80f0: fa fa fa fa 00 00 00 00 00 00[02]fa fa fa fa fa
0x0c0c7fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0c7fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0c7fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0c7fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0c7fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

Shadow byte legend (one shadow byte represents 8 application bytes):

```
Addressable:           00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:      fa
Freed heap region:      fd
Stack left redzone:     f1
Stack mid redzone:      f2
Stack right redzone:    f3
Stack after return:     f5
```

```
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
ASan internal: fe
Left alloca redzone: ca
Right alloca redzone: cb
Shadow gap: cc
==912388==ABORTING
```

## ExpressionCoerceFP in expression.c when called from ExpressionParseFunctionCall in expression.c.

---

File for Reprotuction:

[ExpressionCoerceFP\\_heap\\_overflow.c.zip](#)

```
=====
==912597==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6040000adb8 at pc
0x5555f45b9467 bp 0x7ffcd4551690 sp 0x7ffcd4551688
READ of size 1 at 0x6040000adb8 thread T0
#0 0x5555f45b9466 in ExpressionCoerceFP
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:300
#1 0x5555f45d35c2 in StdioBasePrintf cstdlib/stdio.c:385
#2 0x5555f45d6e9f in StdioPrintf cstdlib/stdio.c:682
#3 0x5555f45c4edd in ExpressionParseFunctionCall
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1909
#4 0x5555f45c237c in ExpressionParse
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1607
#5 0x5555f45b66a0 in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:646
#6 0x5555f45b56c1 in ParseFor /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:524
#7 0x5555f45b6e02 in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:715
#8 0x5555f45b8380 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:897
#9 0x5555f45d0d0e in PicocPlatformScanFile platform/platform_unix.c:129
#10 0x5555f45a7213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
#11 0x7fa48e4d67fc in __libc_start_main ../csu/libc-start.c:332
#12 0x5555f45a6d49 in _start (/home/kali/projects/fuzzing/fuzz_targets/picoc/picoc+0x16d49)

0x6040000adb8 is located 2 bytes to the right of 38-byte region [0x6040000ad90,0x6040000adb6)
allocated by thread T0 here:
#0 0x7fa48e8d1987 in __interceptor_malloc
../../../../src/libsanitizer/asan/asan_malloc_linux.cpp:154
#1 0x5555f45c5b80 in HeapAllocMem /home/kali/projects/fuzzing/fuzz_targets/picoc/heap.c:127
#2 0x5555f45a824a in TableSetIdentifier
/home/kali/projects/fuzzing/fuzz_targets/picoc/table.c:162
#3 0x5555f45a845b in TableStrRegister2
/home/kali/projects/fuzzing/fuzz_targets/picoc/table.c:179
#4 0x5555f45ab965 in LexGetStringConstant
```

```
/home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:390
#5 0x5555f45acc4f in LexScanGetToken /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:502
#6 0x5555f45adfc6 in LexTokenize /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:642
#7 0x5555f45ae527 in LexAnalyse /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:704
#8 0x5555f45b81b7 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:874
#9 0x5555f45d0d0e in PicocPlatformScanFile platform/platform_unix.c:129
#10 0x5555f45a7213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
#11 0x7fa48e4d67fc in __libc_start_main ../csu/libc-start.c:332
```

SUMMARY: AddressSanitizer: heap-buffer-overflow

/home/kali/projects/fuzzing/fuzz\_targets/picoc/expression.c:300 in ExpressionCoerceFP

Shadow bytes around the buggy address:

```
0x0c087fff9560: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
0x0c087fff9570: fa fa 00 00 00 00 01 fa fa fa 00 00 00 00 00 fa
0x0c087fff9580: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
0x0c087fff9590: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
0x0c087fff95a0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
=>0x0c087fff95b0: fa fa 00 00 00 00 06[fa]fa fa 00 00 00 00 00 fa
0x0c087fff95c0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
0x0c087fff95d0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
0x0c087fff95e0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 03 fa
0x0c087fff95f0: fa fa 00 00 00 00 00 05 fa fa 00 00 00 00 00 fa
0x0c087fff9600: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 00
```

Shadow byte legend (one shadow byte represents 8 application bytes):

```
Addressable:           00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:      fa
Freed heap region:      fd
Stack left redzone:     f1
Stack mid redzone:      f2
Stack right redzone:    f3
Stack after return:     f5
Stack use after scope:  f8
Global redzone:         f9
Global init order:      f6
Poisoned by user:       f7
Container overflow:     fc
Array cookie:           ac
Intra object redzone:   bb
ASan internal:          fe
Left alloca redzone:    ca
Right alloca redzone:   cb
Shadow gap:             cc
```

==912597==ABORTING

## StdioOutPutc in cstdlib/stdio.c L64 when called from ExpressionParseFunctionCall in expression.c.

File for Reprotuction:

[StdioOutPutc\\_heap\\_overflow.c.zip](#)

=====

==912677==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6040000aef8 at pc 0x55af1d709269 bp 0x7ffd9cb1bf90 sp 0x7ffd9cb1bf88

WRITE of size 1 at 0x6040000aef8 thread T0

```
#0 0x55af1d709268 in StdioOutPutc cstdlib/stdio.c:64
#1 0x55af1d70baa8 in StdioBasePrintf cstdlib/stdio.c:415
#2 0x55af1d70f768 in StdioSprintf cstdlib/stdio.c:718
#3 0x55af1d6fcedd in ExpressionParseFunctionCall
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1909
#4 0x55af1d6fa37c in ExpressionParse
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1607
#5 0x55af1d6ee6a0 in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:646
#6 0x55af1d6edb07 in ParseBlock /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:558
#7 0x55af1d6ee74b in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:651
#8 0x55af1d6ea028 in ParseStatementMaybeRun
/home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:54
#9 0x55af1d6ed55c in ParseFor /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:504
#10 0x55af1d6eee02 in ParseStatement
/home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:715
#11 0x55af1d6f0380 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:897
#12 0x55af1d708d0e in PicocPlatformScanFile platform/platform_unix.c:129
#13 0x55af1d6df213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
#14 0x7fddae07c7fc in __libc_start_main ../csu/libc-start.c:332
#15 0x55af1d6ded49 in _start (/home/kali/projects/fuzzing/fuzz_targets/picoc/picoc+0x16d49)
```

0x6040000aef8 is located 0 bytes to the right of 40-byte region [0x6040000aed0,0x6040000aef8) allocated by thread T0 here:

```
#0 0x7fddae477987 in __interceptor_calloc
../././././src/libsanitizer/asan/asan_malloc_linux.cpp:154
#1 0x55af1d6fdb80 in HeapAllocMem /home/kali/projects/fuzzing/fuzz_targets/picoc/heap.c:127
#2 0x55af1d7023a9 in VariableAlloc
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:77
#3 0x55af1d702429 in VariableAllocValueAndData
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:97
#4 0x55af1d702701 in VariableAllocValueFromType
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:119
#5 0x55af1d703aa7 in VariableDefine
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:303
#6 0x55af1d7046aa in VariableDefineButIgnoreIdentical
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:383
#7 0x55af1d6ec540 in ParseDeclaration
/home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:366
#8 0x55af1d6eef6e in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:738
#9 0x55af1d6f0380 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:897
#10 0x55af1d708d0e in PicocPlatformScanFile platform/platform_unix.c:129
#11 0x55af1d6df213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
#12 0x7fddae07c7fc in __libc_start_main ../csu/libc-start.c:332
```

SUMMARY: AddressSanitizer: heap-buffer-overflow cstdlib/stdio.c:64 in StdioOutPutc  
Shadow bytes around the buggy address:

```
0x0c087fff9580: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
0x0c087fff9590: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
0x0c087fff95a0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
0x0c087fff95b0: fa fa 00 00 00 00 02 fa fa fa 00 00 00 00 00 fa
0x0c087fff95c0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
```

```

=>0x0c087fff95d0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00[fa]
0x0c087fff95e0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 00
0x0c087fff95f0: fa fa 00 00 00 00 00 fa fa fa fa fa fa fa fa fa
0x0c087fff9600: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c087fff9610: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c087fff9620: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable:          00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:    fa
Freed heap region:    fd
Stack left redzone:    f1
Stack mid redzone:    f2
Stack right redzone:   f3
Stack after return:    f5
Stack use after scope: f8
Global redzone:        f9
Global init order:    f6
Poisoned by user:      f7
Container overflow:    fc
Array cookie:          ac
Intra object redzone:  bb
ASan internal:         fe
Left alloca redzone:   ca
Right alloca redzone:  cb
Shadow gap:            cc
==912677==ABORTING

```

## ExpressionCoerceInteger in expression.c when called from ExpressionInfixOperator in expression.c.

---

File for Reprotuction:

[ExpressionCoerceInteger\\_heap\\_overflow.c.zip](#)

```

=====
==912683==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x606000007d8 at pc
0x56335c8a2b15 bp 0x7ffe99b322b0 sp 0x7ffe99b322a8
READ of size 4 at 0x606000007d8 thread T0
#0 0x56335c8a2b14 in ExpressionCoerceInteger
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:242
#1 0x56335c8a9028 in ExpressionInfixOperator
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1007
#2 0x56335c8aa85c in ExpressionStackCollapse
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1316
#3 0x56335c8acc7b in ExpressionParse
/home/kali/projects/fuzzing/fuzz_targets/picoc/expression.c:1684
#4 0x56335c8a06a0 in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:646
#5 0x56335c8a2380 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:897
#6 0x56335c8bad0e in PicocPlatformScanFile platform/platform_unix.c:129
#7 0x56335c891213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62

```

```
#8 0x7fefac2b7fc in __libc_start_main ../csu/libc-start.c:332
#9 0x56335c890d49 in _start (/home/kali/projects/fuzzing/fuzz_targets/picoc/picoc+0x16d49)
```

0x606000007d8 is located 0 bytes to the right of 56-byte region [0x606000007a0,0x606000007d8) allocated by thread T0 here:

```
#0 0x7fefac26987 in __interceptor_calloc
.././././././src/libsanitizer/asan/asan_malloc_linux.cpp:154
#1 0x56335c8afb80 in HeapAllocMem /home/kali/projects/fuzzing/fuzz_targets/picoc/heap.c:127
#2 0x56335c8b43a9 in VariableAlloc
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:77
#3 0x56335c8b4429 in VariableAllocValueAndData
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:97
#4 0x56335c8b4701 in VariableAllocValueFromType
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:119
#5 0x56335c8b5aa7 in VariableDefine
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:303
#6 0x56335c8b66aa in VariableDefineButIgnoreIdentical
/home/kali/projects/fuzzing/fuzz_targets/picoc/variable.c:383
#7 0x56335c89e540 in ParseDeclaration
/home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:366
#8 0x56335c8a0f6e in ParseStatement /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:738
#9 0x56335c8a2380 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:897
#10 0x56335c8bad0e in PicocPlatformScanFile platform/platform_unix.c:129
#11 0x56335c891213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
#12 0x7fefac2b7fc in __libc_start_main ../csu/libc-start.c:332
```

SUMMARY: AddressSanitizer: heap-buffer-overflow

/home/kali/projects/fuzzing/fuzz\_targets/picoc/expression.c:242 in ExpressionCoerceInteger

Shadow bytes around the buggy address:

```
0x0c0c7fff80a0: fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
0x0c0c7fff80b0: fd fd fd fa fa fa fa fa fd fd fd fd fd fd fd fa
0x0c0c7fff80c0: fa fa fa fa fd fd fd fd fd fd fd fa fa fa fa fa
0x0c0c7fff80d0: 00 00 00 00 00 00 06 fa fa fa fa fa 00 00 00 00
0x0c0c7fff80e0: 00 00 00 00 fa fa fa fa 00 00 00 00 00 00 00 00
=>0x0c0c7fff80f0: fa fa fa fa 00 00 00 00 00 00 00 00[fa]fa fa fa fa
0x0c0c7fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0c7fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0c7fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0c7fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0c7fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

Shadow byte legend (one shadow byte represents 8 application bytes):

```
Addressable:             00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:       fa
Freed heap region:       fd
Stack left redzone:      f1
Stack mid redzone:       f2
Stack right redzone:     f3
Stack after return:      f5
Stack use after scope:   f8
Global redzone:          f9
Global init order:       f6
Poisoned by user:        f7
Container overflow:      fc
Array cookie:            ac
Intra object redzone:    bb
```

```
ASan internal:      fe
Left alloca redzone: ca
Right alloca redzone: cb
Shadow gap:        cc
==912683==ABORTING
```

## LexSkipComment in lex.c when called from LexScanGetToken in lex.c.

File for Reprotuction:

[LexSkipComment\\_heap\\_overflow.c.zip](#)

```
=====
==912887==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60c0000000b9 at pc
0x55736f5b3e90 bp 0x7ffe3e509790 sp 0x7ffe3e509788
READ of size 1 at 0x60c0000000b9 thread T0
#0 0x55736f5b3e8f in LexSkipComment /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:430
#1 0x55736f5b521c in LexScanGetToken /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:532
#2 0x55736f5b5fc6 in LexTokenize /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:642
#3 0x55736f5b6527 in LexAnalyse /home/kali/projects/fuzzing/fuzz_targets/picoc/lex.c:704
#4 0x55736f5c01b7 in PicocParse /home/kali/projects/fuzzing/fuzz_targets/picoc/parse.c:874
#5 0x55736f5d8d0e in PicocPlatformScanFile platform/platform_unix.c:129
#6 0x55736f5af213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
#7 0x7f22e68a87fc in __libc_start_main ../csu/libc-start.c:332
#8 0x55736f5aed49 in _start (/home/kali/projects/fuzzing/fuzz_targets/picoc/picoc+0x16d49)
```

0x60c0000000b9 is located 0 bytes to the right of 121-byte region [0x60c000000040,0x60c0000000b9) allocated by thread T0 here:

```
#0 0x7f22e6ca37cf in __interceptor_malloc
../../../../src/libsanitizer/asan/asan_malloc_linux.cpp:145
#1 0x55736f5d88a7 in PlatformReadFile platform/platform_unix.c:94
#2 0x55736f5d8bfc in PicocPlatformScanFile platform/platform_unix.c:121
#3 0x55736f5af213 in main /home/kali/projects/fuzzing/fuzz_targets/picoc/picoc.c:62
#4 0x7f22e68a87fc in __libc_start_main ../csu/libc-start.c:332
```

SUMMARY: AddressSanitizer: heap-buffer-overflow  
/home/kali/projects/fuzzing/fuzz\_targets/picoc/lex.c:430 in LexSkipComment  
Shadow bytes around the buggy address:

```
0x0c187fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c187fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c187fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c187fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c187fff8000: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00
=>0x0c187fff8010: 00 00 00 00 00 00 00 [01]fa fa fa fa fa fa fa fa
0x0c187fff8020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05
0x0c187fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c187fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c187fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c187fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

Shadow byte legend (one shadow byte represents 8 application bytes):

```
Addressable:      00
Partially addressable: 01 02 03 04 05 06 07
```



```
Heap left redzone:      fa
Freed heap region:      fd
Stack left redzone:     f1
Stack mid redzone:      f2
Stack right redzone:    f3
Stack after return:     f5
Stack use after scope:  f8
Global redzone:         f9
Global init order:      f6
Poisoned by user:       f7
Container overflow:     fc
Array cookie:           ac
Intra object redzone:   bb
ASan internal:          fe
Left alloca redzone:    ca
Right alloca redzone:   cb
Shadow gap:             cc
==912887==ABORTING
```

#### Assignees

No one assigned

---

#### Labels

None yet

---

#### Projects

None yet

---

#### Milestone

No milestone

---

#### Development

No branches or pull requests

---

1 participant

