

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

# PICOC Null Pointer Dereference Denial of Service #34

[Open](#)

Halcy0nic opened this issue on Jun 21 · 1 comment

Halcy0nic commented on Jun 21

PICOC Suffers from a Denial of Service (CWE476) vulnerability as a result of a Null Pointer Dereference. Any project or library that uses Picoc also suffers from this issue. An example of this would be picoc-js (<https://www.npmjs.com/package/picoc-js>). As a result PICOC will immediately segfault.

## Reproduction Steps

1. Create a file to be executed by the PICOC interpreter

```
$ touch vulncode
```

2. Add the following code to the file:

```
printf("Before Crash\n");  
**4%;  
printf("This code won't execute because of the crash\n");
```

3. Execute PICOC against the file:

```
$ ./picoc -s vulncode
```

4. You will receive a segfault and the program will crash. This is a result of a null pointer dereference that is not caught or handled by the interpreter. The vulnerable line of code can be seen below:

```
**4%;
```

# Solution

Adding a few if statements that verify the pointer is not NULL before usage will solve this problem. You can find more information about this here:

[https://owasp.org/www-community/vulnerabilities/Null\\_Dereference](https://owasp.org/www-community/vulnerabilities/Null_Dereference)

Halcy0nic commented on Jul 6

Author

## GDB Trace:

```
Starting program: /home/kali/projects/fuzzing/picoc/picoc vuln/crash1
Program received signal SIGSEGV, Segmentation fault.
VariableDereferencePointer (PointerValue=0x62d2b8, DereferVal=0x7fffffff580, DereferOffset=0x7fffffff58c, DereferType=0x7fffffff578, DereferIsValue=0x7fffffff588) at variable.c:519
519      DereferType = PointerValue->Type->FromType;
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA

[ REGISTERS ]
RAX 0x0
RBX 0x0
RCX 0x7fffffff578 ← 0x0
RDX 0x7fffffff58c ← 0x62d2b800000000
RDI 0x62d2b8 ← 0x0
RSI 0x7fffffff580 ← 0x0
R8 0x7fffffff588 ← 0x1
R9 0x0
R10 0xffffffffffff90d
R11 0x20
R12 0x400c00 (_start) ← xor ebp, ebp
R13 0x0
R14 0x0
R15 0x0
RBP 0x7fffffff540 → 0x7fffffff5a0 → 0x7fffffff620 → 0x7fffffff680 → 0x7fffffff7d0 ← ...
RSP 0x7fffffff540 → 0x7fffffff5a0 → 0x7fffffff620 → 0x7fffffff680 → 0x7fffffff7d0 ← ...
RIP 0x413fab (VariableDereferencePointer+56) ← mov rdx, qword ptr [rax + 0x18]

[ DISASM ]
> 0x413fa0 <VariableDereferencePointer+56> mov rdx, qword ptr [rax + 0x18]
0x413fa4 <VariableDereferencePointer+60> mov rax, qword ptr [rbp - 0x20]
0x413fa8 <VariableDereferencePointer+64> mov qword ptr [rax], rdx
0x413fab <VariableDereferencePointer+67> cmp qword ptr [rbp - 0x18], 0
0x413fb0 <VariableDereferencePointer+72> je VariableDereferencePointer+84 <VariableDereferencePointer+84>
↓
0x413fbc <VariableDereferencePointer+84> cmp qword ptr [rbp - 0x28], 0
0x413fc1 <VariableDereferencePointer+89> je VariableDereferencePointer+101 <VariableDereferencePointer+101>
↓
0x413fcd <VariableDereferencePointer+101> mov rax, qword ptr [rbp - 8]
0x413fd1 <VariableDereferencePointer+105> mov rax, qword ptr [rax + 8]
0x413fd5 <VariableDereferencePointer+109> mov rax, qword ptr [rax]
0x413fd8 <VariableDereferencePointer+112> pop rbp
↓ counter / popcnt 1
```

## Assignees

No one assigned

## Labels

None yet

## Projects

None yet

## Milestone

No milestone

## Development

No branches or pull requests

1 participant

