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%;
```

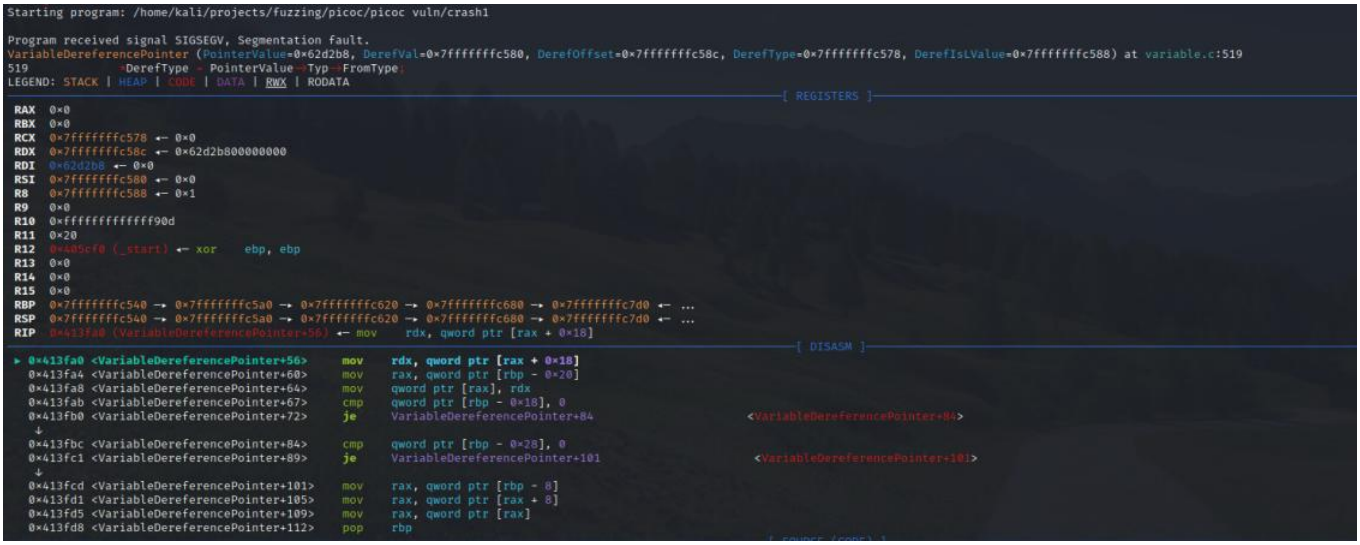
Solution

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

Halcy0nic commented on Jul 6 — Author

GDB Trace:



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant