Open Issue created 5 months ago by Halcy0nic

PICOC Null Pointer Dereference Denial of Service

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

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. More information

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Link issues together to show that they're related or that one is blocking others. Learn more.

Activity

Halcy0nic @Halcy0nic · 4 months ago Author

GDB Trace: