Software Assurance Tips

A product of the Software Assurance Tips Team[2]

Jon Hood

Monday 13th September, 2021

1 Static Header Paths

Updated Monday 13th September, 2021

While manually reviewing some VxWorks-based code, I noticed that a developer had included a header file from the VxWorks library in an odd way. The entire path to the header file is present in the include directive as shown in Listing 1.

```
#include <C:\VxWorks Headers version\path\to\staticdefinitions.h>
```

Listing 1: Include Directive

Static paths inside of source code, particularly in the headers, can cause several issues.

First, the code can only be compiled on an OS That understands the path directives. Non-ubiquitous code is flagged, particularly when the software itself is written to support any platform within the VxWorks portfolio.[1] Note that the C99 standard allows `#include` directives with \ as a directory separator when it's between either <> or "".

Second, the VxWorks-Headers-version folder is not maintained in version control. It is part of the build environment, but that environment has several different versions of VxWorks updates installed. An update to VxWorks means that the code files themselves have to be updated to support the new VxWorks version.

Finally, the VxWorks libraries are installed with any-user privileges that allow an attacker with access to the build environment to inject code into the header file in a way that avoids the scan tools being used. Since the potentially injected code is never a apart of the code repository, it avoids peer review, scrutiny, and change management.

Attacking the build environment of a product is one of the sneakiest ways to inject malicious software into it. Developers who rely on external code should verify that it's trusted, under change management, and scanned as part of their solution.

References

[1] CWE Content Team. “CWE-589: Call to Non-ubiquitous API”. In: (2021). URL: https://cwe.mitre.org/data/definitions/589.html.

[2] Jon Hood, ed. SwATips. https://www.SwATips.com/.