A Response to Comments on the C Annex of TR 24772

David Keaton, CERT

2011-10-14

These notes are submitted for consideration as a response to the comments dated 2011-09-29 on the C Annex of the Vulnerabilities TR 24772.

C.1 (actually C.3.1)

Regarding typedefs, the comment is correct that no type safety is provided. A common idiom is to wrap the data in a structure, as follows, which does provide type safety.

```
struct Celsius { double value; };
```

Therefore, section C.3.1 is correct that C is both strongly and weakly typed, and no change is needed.

C.18 (C.XZI)

The vulnerability applies to languages where sign extension is not enforced by the type system. No change is needed.

C.20 (C.WXQ)

Thanks to the submitter for the detailed review, which uncovered this omission.

The WXQ section was added to the main part of the document after the C annex was written, and then not updated in the annex except for a place holder. This section needs to be filled in.

C.23 (C.BJL)

Header files do not create a separate name space.

The vulnerability applies to languages that provide a user-controlled ordering of name spaces. C lacks this feature. No change is needed to the annex. There will be a proposal to update the main body of the TR to make this clearer.

C.25 (C.JCW)

Section C.25 acknowledges this issue, and suggests using parentheses to mitigate it. No change is needed.