ISO/IEC JTC 1/SC 22/OWGV N 0217

Revised format for language-specific annexes

After comparing the treatments of the different examples, Meeting 11 concluded that the vulnerability descriptions in the language-specific annexes should have the following format:

Annex <language>

(informative)

Vulnerability descriptions for <language>

<language>.1 Identification of standards

[This section should list the relevant language standards and other documents that describe the language treated in the annex. It should not be simply a list of standards. It should do whatever is required to describe the language that is the baseline. In some cases, it might be a standard plus some other documents, or a standard minus the annex that lists deprecated features. It might include some explanation, such as "don't use any features that are undefined".]

<language>.2 General terminology and concepts

[This section should provide an overview of general terminology and concepts that are utilized throughout the annex.]

Every vulnerability description of Clause 6 of the main document should be addressed in the annex in the same order even if there is simply a notation that it is not relevant to the language in question.

Each vulnerability description should have the following format:

<language>.<x> <Vulnerability Name> [<3 letter tag>]

<language>.<x>.0 Status and history
[Revision history. This section will eventually be removed.]
<language>.<x>.1 Terminology and features
[In this and other sections, if there is nothing to be explained, simply say "None".]
[This section should describe terms that are in the language standard and which are used in the explanation that follows.]
term: An explanation in the form of one or more complete sentences.
…
<language>.<x>.2 Description of vulnerability
[This merges the prior sections for description and mechanism. Examples, both good and bad, are strongly encouraged.]
<language>.<x>.3 Avoiding the vulnerability or mitigating its effects
- [An imperative sentence followed by optional additional sentences written in the indicative.]
- …

<language>.<x>.4 Implications for standardization
Future standardization efforts should consider:
- Requiring ...
- Adding ...
- Changing ...
- Other verbs ending in "ing"

<language>.<x>.5 Bibliography
[No change from the current]

In those cases where a vulnerability is simply not applicable to the language, the following format should be used:

<language>.<x> <Vulnerability Name> [<3 letter tag>]

This vulnerability is not applicable to <language>. [Optionally, an explanation of inapplicability may be added, including qualifications and pointers to other related vulnerabilities that might be present.]