Analysis of the delta of the Core Document between Edition 1 (N0268), Edition 2 (N0436) and current Baseline (N0461), including the impact on the Ada Annex

(contributed by Erhard Ploedereder)

Section 7 is ignored in this analysis, since the annexes do not discuss these vulnerabilities.

Document structure and additional sections:

Some sections have been moved but the Ada Annex has been changed accordingly, so no addition structural work is needed in the Ada Annex.

The "Additional Vulnerabilities" in Section 8 of Edition 2, in N0461 added as subsections 6.58 – 6.63, as well as two new subsections 6.64 and 6.65 from the area of security, are yet to have counterparts produced for the Ada Annex (and probably all other annexes).

Content changes in subsections:

Subsections that are unchanged or with editorial changes only:

3, 4, 8, 11, 12, 13, 14, 15, 25, 26, 27, 30, 31, 32, 33, 34, 35, 36, 37, 39, 40, 41, 44, 47, 48, 49, 50, 53, 54, 55, 56, 57

Wording changes that are very unlikely to have any effect on the Ada annex (but may have on other annexes):

5, 7, 10, 28, 45

Additional subsections in the above categories, but moved to a different place (in Ada Annex moved as well):

19-24 (23 has wording changes that might affect other annexes), 42, 43, 58-63

Subsections with changes that affect the Ada annex and possibly other annexes:

6: Completeness checks in cases/switches moved to subsection 29; Ada annex needs a deletion of these completeness checks at the end of C.6.1 (since covered in C.29)

21: the explanation of the vulnerability has changed; check annexes for consistency; Ada annex should drop advice about dead store (and may-be simplify the advice, since the PigCounter example is not very convincing).

38: section was completely rewritten; the Ada annex is too shallow to address all the issues raised

Subsections with changes that likely affect the contents of annexes, but do not for the Ada annex:

9: A merger of two vulnerabilities; basically a new write-up, some annexes may need fixes

16: A (partial?) merger; annexes need review

17: New; split mainly from the old version of 16; annexes need review

18 : New; no recognizable origin but related to 16+17; annexes need review

29: Added the completeness checks from 6; annexes need review

46: New; annexes need review

51: New; annexes need review

52: New; annexes need review

Core problems:

21 is badly rewritten from the old 10 -- repetitive "Mechanism of"-section

6.46.3 has an off-by-one error in the C code (10->9, since Pascal starts counting at 1)

6.59/8.4.1 the subsection reference at the end has not been corrected as part of the transfer, but has been deleted.

==========

Notes: old 6.9 in Ed. 1 (issues with file names) has been deleted