ISO/IEC JTC 1/SC 22/WG 23 N 0281

Markup of extract of N0275, draft language-specific annex for SPARK

Date 16 September 2010

Contributed by SC 22/WG 9

Original file name

Notes Extract of N 0275 with markups made using Track Changes

1

1		46 47 48	Both of these properties can be checked by static analysis. Static analysis can be used to check for <whatever cases="" remain="">.</whatever>
2 3 4	SPARK.3.CSJ Passing Parameters and Return Values [CSJ]	49 50	SPARK.3.CSJ.4 Implications for standardization
5	[Here's an example of how to modify a description of a mitigation.]	51	None.
6 7 8	SPARK mitigates this vulnerability.	52 53	SPARK.3.CSJ.5 Bibliography None.
9	SPARK.3.CSJ.1 Terminology		SPARK.3.DCM Dangling
10	and features	55	References to Stack Frames
11	As in Ada.CSJ.1.	56	[DCM]
12	SPARK.3.CSJ.2 Description of vulnerability	57 58 59	[The suggested treatment of prevented vulnerabilities is as shown in this example.]
13 14	As in Ada.CSJ.3. SPARK goes further than	60	SPARK prevents this vulnerability by
15 16	Ada with regard to this vulnerability. Specifically:	61 62	forbidding the use of the 'Address and 'Access attributes of Ada
17	ODADIK forbide all alianian of	63	SPARK.3.DCM.1 Terminology
18 19	 SPARK forbids all aliasing of parameters and names [SLRM 6]. 	64	and features
20 21	SPARK is designed to offer	65	As in Ada.3.DCM.1.
22 23	consistent semantics regardless of the parameter passing mechanism	66	SPARK.3.DCM.2 Description of
24	employed by a particular compiler.	67	vulnerability
25	Thus this implementation-dependent	68	As in Ada.3.DCM.2.
26 27	behaviour of Ada is eliminated from SPARK.		
28	<u>5.7</u>	69	SPARK.3.DCM.3 Avoiding the
		70	vulnerability or mitigating its
29	SPARK.3.CSJ.3 Avoiding the	71	effects
30	vulnerability or mitigating its effects	72	SPARK forbids the use of the 'Address
31		73 74	attribute to read the address of an object [SLRM 4.1]. The 'Access attribute and all
32 33	SPARK goes further than Ada with regard to this vulnerability. Specifically:	75	access types are also forbidden, so this
34	нь чинегаршту. Эреспьану.	76	vulnerability cannot occur.
35	 SPARK forbids all aliasing of 	77	SPARK.3.DCM.4 Implications
36 37	parameters and names [SLRM 6].	77 78	for standardization
38	 SPARK is designed to offer 		
39	consistent semantics regardless of	79	None.
40 41	the parameter passing mechanism employed by a particular compiler.	80	SPARK.3.DCM.5 Bibliography
42	Thus this implementation-dependent	81	None.
43	behaviour of Ada is eliminated from	82	Tono.
44 45	SPARK.	83	