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

SPARK.3.CSJ Passing Parameters and Return Values [CSJ]

[Here's an example of how to modify a description of a mitigation.]

SPARK mitigates this vulnerability.

SPARK.3.CSJ.1 Terminology and features

As in Ada.CSJ.1.

SPARK.3.CSJ.2 Description of vulnerability

As in Ada.CSJ.3. SPARK goes further than Ada with regard to this vulnerability. Specifically:

- SPARK forbids all aliasing of parameters and names [SLRM 6].
- SPARK is designed to offer consistent semantics regardless of the parameter passing mechanism employed by a particular compiler. Thus this implementation-dependent behaviour of Ada is eliminated from SPARK.

SPARK.3.CSJ.3 Avoiding the vulnerability or mitigating its effects

~~SPARK goes further than Ada with regard to this vulnerability. Specifically:~~

- ~~SPARK forbids all aliasing of parameters and names [SLRM 6].~~
- ~~SPARK is designed to offer consistent semantics regardless of the parameter passing mechanism employed by a particular compiler. Thus this implementation-dependent behaviour of Ada is eliminated from SPARK.~~

~~Both of these properties can be checked by static analysis.~~Static analysis can be used to check for <whatever cases remain>.

SPARK.3.CSJ.4 Implications for standardization

None.

SPARK.3.CSJ.5 Bibliography

None.

SPARK.3.DCM Dangling References to Stack Frames [DCM]

[The suggested treatment of prevented vulnerabilities is as shown in this example.]

SPARK prevents this vulnerability by forbidding the use of the 'Address and 'Access attributes of Ada.~~.~~

~~SPARK.3.DCM.1 Terminology and features~~

~~As in Ada.3.DCM.1.~~

~~SPARK.3.DCM.2 Description of vulnerability~~

~~As in Ada.3.DCM.2.~~

~~SPARK.3.DCM.3 Avoiding the vulnerability or mitigating its effects~~

~~SPARK forbids the use of the 'Address attribute to read the address of an object [SLRM 4.1]. The 'Access attribute and all access types are also forbidden, so this vulnerability cannot occur.~~

~~SPARK.3.DCM.4 Implications for standardization~~

~~None.~~

~~SPARK.3.DCM.5 Bibliography~~

~~None.~~