Business Plan and Convener's Report

ISO/IEC/JTC 1/SC 22/WG 23 (Programming Language Vulnerabilities)

Document: ISO/IEC JTC 1/SC 22/WG 23/N0547

Stephen Michell 2017-2-20 9:22 AM
Deleted: 11

Date: 2015-06-09

PERIOD COVERED: July 2014 – July 2015

SUBMTTED BY:

Convener, ISO/IEC JTC 1/SC 22/WG 23: Vulnerabilities
Stephen Michell
Maurya Software Inc
1969 Rosebella Ave
Ottawa, Ontario, Canada K1T 1G6

Office: +1(613)299-9047
E-mail: stephen.michell@maurya.on.ca

1. MANAGEMENT SUMMARY

1.1. JTC 1/SC 22/WG 23 Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use

1.2. PROJECT REPORT

1.2.1. COMPLETED PROJECTS

ISO/IEC TR 24772:2012, *Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection*. This is a Technical Report.

1.2.2. PROJECTS UNDERWAY

JTC 1 NP 24772, *Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection*. This is the 3rd edition.

JTC 1 NP 17960, *Code Signing for Source Code*. This project is to produce an International Standard, and currently is in DIS ballot.

1.2.3. CANCELLED PROJECTS

None over this time period.

1.2.4. COOPERATION and COMPETITION

Where appropriate, WG 23 has established active liaisons with other SC22 working groups, other JTC 1 subcommittee working groups (such as SC 27/WG 3 and SC 7 WG19) and other standards organizations, such as Ecma International. See the table in 2.3 for a list of liaisons.

There is no apparent direct competition with any other current SC22 working group or JTC 1 subcommittee.

2. PERIOD REVIEW

2.1. MARKET REQUIREMENTS

WG 23 is responding to the needs of the programming language community by inclusion. WG 23 will accept input and liaison by any and all appropriate organizations.

The marketplace demands robust, secure software. Vulnerabilities are the antithesis of robust, secure software. Many of the attacks on software-based systems succeed because the computer language used did not prevent the attack vector, and did not warn the developer that the code being produced contained flaws that could be used to generate attacks.

WG 23 has produced 2 editions of TR 24772, but there are vulnerabilities that still need to be identified, and programming languages that still need to be documented with regards to vulnerabilities.

2.2. ACHIEVEMENTS

WG 23 has published the second edition of TR 24772, and started work on the third edition.

WG 23 worked on the 17960 project, a second CD ballot, and a DIS ballot which concluded with unanimous approval without comments, see SC 22 N4981.

2.3. RESOURCES

Five national bodies are currently participating in the most recent teleconference meeting: Canada, Italy, Japan, Spain, UK, and the USA, as well as several liaisons.

Over the last several years WG 23 has made Web conferencing capabilities available for those that are finding it difficult to travel. WG 23 would like to thank ISO for the Web conferencing support.

Liaison with five SC22 Language groups, and four groups outside of SC22 has been established. Liaisons fill a valuable role in that they identify the vulnerabilities that exist (and do not exist) in their language, produce the primary documentation of those vulnerabilities and turn them into the relevant language-dependent part in conjunction with the core team through the liaison individual.

Current WG 23 liaisons are:

Group	Name/Type	Person assigned
SC 22/WG4	Cobol	Robert Karlin, Chris Tandy
SC 22/WG5	Fortran	Dan Nagle
SC 22/WG9	Ada	Erhard Ploedereder
SC 22/ WG14	C	Clive Pygott
SC 22/ WG 21	C++	Group
SC 7/WG 19	Open Distributed Processing and Modeling Languages	Cesar Gonzalez-Perez
SC 27/WG 3	Security evaluation, testing and specification	Tatsuaki Takebe

ECMA TC39/TG2	C#	Nomination pending
JSR-282/JSR-302	Real-Time/Safety-Critical-Java	Ben Brosgol
Linux Foundation	Linux	Nick Stoughton
MDC	MUMPS	Ed de Moel

3. FOCUS NEXT WORK PERIOD

. 3.1. DELIVERABLES

None for this time period.

. 3.2. STRATEGIES

. WG 23 has decided that a core document and seven language-specific annexes, with at least two or three more in planning, creates a maintenance burden that makes it difficult to keep all portions of the document up to date in a single document.

. WG 23 has therefore decided to split TR 24772 into a series of parts, as follows (see also clause 4.1 for the official request for SC 22 action):

TR24772-1 Information Technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use – Language Independent View

TR24772-2 Information Technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use – Programming Language Ada

TR24772-3 Information Technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use – Programming Language C

TR24772-4 Information Technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages

through language selection and use – Programming Language Python

TR24772-5 Information Technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use – Programming Language Ruby

TR24772-6 Information Technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use – Programming Language Spark

TR24772-7 Information Technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use – Programming Language PHP

TR24772-8 Information Technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use – Programming Language Fortran

TR24772-9 Information Technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use – Programming Language COBOL

3.3. RISKS

The loss of the previous convenor/editor created a significant loss of expertise and resource for the group, as the remaining members are volunteers instead of funded to do the work. WG 23 has responded by separating the role of convenor and editor for TR 24772, and will assigned different editors to each language-specific part as maintenance to it is initiated.

3.4. OPPORTUNITIES

No special opportunities arise during the next year.

3.5. WORK PROGRAM PRIORITIES

See 4.1.

4. OTHER ITEMS

4.1. POSSIBLE ACTION REQUESTS AT FORTHCOMING PLENARY

WG 23 requests that SC 22 approve a program split of 22.24772 into projects as specified in clause 3.2.

22.24772-1 Language independent,

22.24772-2 Ada,

22.24772-3 C,

22.24772-4 Python,

22.24772-5 Ruby,

22.24772-6 PHP,

22.24772-7 Spark,

22.24772-8 Fortran, and

22.24772-9 COBOL

WG 23 requests that SC 22 initiate the maintenance of TR 24772 as project 22.24772-1. This project will be a project of 36 months.

WG 23 requests that SC 22 initiate the maintenance of TR 24772 Annex C Ada as project 22.24772-2. This project will be a project of 36 months.

WG 23 requests that SC 22 initiate the addition of the language-specific part for Programming Language Fortran as project 22.24772-8. This project will be a project of 36 months.

WG 23 requests that SC 22 initiate the addition of the language-specific part for Programming Language Python as project 22.24772-4. This project will be a project of 36 months.

4.2. PROJECT EDITOR The following individuals have been appointed project editors and backup project editors:

- JTC 1 NP 24772-1, Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection. (Project Editor Larry Wagoner, backup Project Editor Clive Pygott)

- JTC 1 NP 17960, Code Signing for Source Code. Larry Wagoner (Project Editor), backup Project Editor vacant

4.3. ELECTRONIC DOCUMENT DISTRIBUTION

WG 23 has conducted some of its detailed technical discussion using the email reflector maintained by Keld Simonsen. WG 23 also has an ftp and Web site at http://open-std.org/sc22/wg23. WG 23 is providing all the appropriate committee documents on the Committee Web site, eliminating the need for paper mailings.

4.4. RECENT MEETINGS

No	Date	Place	Host
20	14-16 Dec 2011	Washington, DC, US	INCITS
21	28-30 Mar 2012	Ottawa, Ontario, CA	SCC
22	20-22 Jun 2012	Stuttgart, DE USA	Universität Stuttgart

23	12-14 Sep 2012	Geneva, CH	IEC
24	12-14 Dec 2012	Teleconference	ISO
25	13-15 Mar 2013	New York, NY	ANSI/INCITS & Blue Pilot
26	08-10 Jun 2013	Berlin, DE	Ada Europe
27	18-21 Sep 2013	Tokyo, Japan	ITSCJ
28	08 Jul 2014	Teleconference	ISO
29	20 Oct 2014	Teleconference	ISO
30	10 Nov 2014	Teleconference	ISO
31	26-27 Jan 2015	Kemah, Tx, USA	Maurya Software Inc
32	26 Feb 2015	Teleconference	ISO
33	30 March 2015	Teleconference	ISO
34	27 April 2015	Teleconference (cancelled)	ISO
35	25 May 2015	Teleconference	ISO
36	26-27 Jun 2015	Madrid, Spain	Ada Europe

4.5. FUTURE MEETINGS

#37 Washington, DC 21 September 2015

#38 New Delhi, India 27-29 October 2015 with SC 27

#39 Teleconference 23 November 2015

#40 Teleconference 14 December 2015

#41 Teleconference 25 January 2015

#42 Teleconference 22 February 2015

#43 London, UK 15-16 April 2015 with WG 14

#44 TBD June 2016

#45 TBD September 2016 with SC 22

#46 Teleconference October 2016

#47 Teleconference November 2016