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/N0797

Date: 2018-06-06

PERIOD COVERED: July 2017 – June 2018

SUBMTTED BY:

Convener, ISO/IEC JTC 1/SC 22/WG 23: Vulnerabilities
Stephen Michell
CSA Group

155 Queen St, Suite 1300
Ottawa, Ontario K1P 6L1 Canada

Office: +1(613)565-5151 x59222
E-mail: stephen.michell@csagroup.org

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 TR 24772:2013, *Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and use*. This is a Technical Report.

ISO/IEC 17960, *Code Signing for Source Code*. This project is to produce an International Standard, and has been published.

1.2.2. PROJECTS UNDERWAY

ISO/IEC TR 24772-1, *Guidance to Avoiding Vulnerabilities in Programming Languages*. This is the update of TR24772:2013 for language independent

vulnerabilities, following the project split of project 22.24772.

ISO/IEC TR 24772-2, *Guidance to Avoiding Vulnerabilities in Programming Languages – Part 2, Vulnerability descriptions for programming language Ada*. This is the update of TR 24772:2013 Annex C for language specific vulnerabilities for Ada, following the project split of project 22.24772.

ISO/IEC TR 24772-3, *Guidance to Avoiding Vulnerabilities in Programming Languages – Part 3, Vulnerability descriptions for programming language C*. This is the update of TR24772:2013 Annex D for language specific vulnerabilities for C, following the project split of project 22.24772.

ISO/IEC TR 24772-4, *Guidance to Avoiding Vulnerabilities in Programming Languages – Part 4, Vulnerability descriptions for programming language Python*. This is the update of TR24772:2013 Annex E for language specific vulnerabilities for Python, following the project split of project 22.24772.

ISO/IEC TR 24772-8, *Guidance to Avoiding Vulnerabilities in Programming Languages – Part 8, Vulnerability descriptions for programming language Fortran*. This is a new Part for language specific vulnerabilities for Fortran.

ISO/IEC TR 24772-9, *Guidance to Avoiding Vulnerabilities in Programming Languages – Part 9, Vulnerability descriptions for programming language C++*. This is a new Part for language specific vulnerabilities for C++.

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 are have made significant progress on the third edition, after splitting the project and the TR into Part 1, language independent part, and Parts 2, 3, 4 and 8 for language-specific vulnerability descriptions for Ada, C, Python, and Fortran. Note that this third edition will be listed as the first edition of TR 24772-1, -2, etc.

2.3. RESOURCES

Seven national bodies have participated in the WG 23 meetings this year: Austria, Canada, China, Italy, Korea, 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. At a typical WG 23, one-third to one-half of all participates are remote, but still participate meaningfully in the meeting. WG 23 finds that mixed-mode meetings work well in developing technical content. WG 23 would like to thank ISO for the Web conferencing support.

Liaison with five SC22 Language groups, and four groups outside of SC22 have 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		Gary Klimowicz
SC 22/WG9		Ada		Erhard Ploedereder
SC 22/ WG14		C		Clive Pygott
SC 22/ WG 21		C++		Group
SC 27/WG 3		Security evaluation, testing and specification		Stephen Michell
ECMA TC39/TG2		C#		No liaison
JSR-282/JSR-302		Real-Time/Safety-Critical-Java		No Liaison
Linux Foundation		Linux		No Liaison, terminate
MDC		MUMPS		No Liaison, terminate

3. FOCUS NEXT WORK PERIOD

3.1. DELIVERABLES

WG 23 plans to submit the following documents for DTR ballot before the SC 22 2018 Plenary:

JTC 1 24772-1, *Guidance to Avoiding Vulnerabilities in Programming Languages*.

JTC 1 24772-2, *Guidance to Avoiding Vulnerabilities in Programming Languages – Part 2, Vulnerability descriptions for programming language Ada*.

JTC 1 24772-3, *Guidance to Avoiding Vulnerabilities in Programming Languages – Part 3, Vulnerability descriptions for programming language C*.

JTC 1 24772-4, *Guidance to Avoiding Vulnerabilities in Programming Languages – Part 4, Vulnerability descriptions for programming language Python*.

For the 2018 SC 22 Plenary WG 23 will propose additional Parts for progress to publication.

3.2. STRATEGIES

WG 23 decided in 2015 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 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
- TR24772-9 Information Technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use – Programming Language C++.

At the 2015 SC 22 plenary, projects for TR24772-1, 2, 3, 4 and 8 were initiated.

3.3. RISKS

Progress on parts 1, 2, 3, 4 and 8 for which work items are allocated are showing reasonable progress. Some of the other parts for which work items have not been initiated require the identification of resources within other working groups or external experts to undertake the work.

3.4. OPPORTUNITIES

No special opportunities arose during the past year.

3.5. WORK PROGRAM PRIORITIES

See 4.1.

4. OTHER ITEMS

4.1. POSSIBLE ACTION REQUESTS AT FORTHCOMING 2017 PLENARY

WG 23 requests the following Liaisons be terminated:

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 and use. (Project Editor Stephen Michell)

- JTC 1 NP 24772-2, Guidance to avoiding vulnerabilities in programming languages through language selection and use – Programming language Ada. (Project Editor Joyce Tokar)

- JTC 1 NP 24772-3, Guidance to avoiding vulnerabilities in programming languages through language selection and use – Programming language C. (Project Editor Clive Pygott, backup Stephen Michell)

- JTC 1 NP 24772-4, Guidance to avoiding vulnerabilities in programming languages through language selection and use – Programming language Python. (Project Editor Stephen Michell)

- JTC 1 NP 24772-8, Guidance to avoiding vulnerabilities in programming languages through language selection and use – Programming language Fortran. (Project Editor Gary Klimowicz)

- JTC 1 NP 17960, Code Signing for Source Code. Stephen Michell (Project Editor).

4.3. ELECTRONIC DOCUMENT DISTRIBUTION

Documents relevant to ISO/IEC/JTC1/SC22 processing are being entered on the ISO eCommittee web site for WG 23. WG 23 conducts 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.

4.4. RECENT MEETINGS

No	Date	Place	# attendees	Host
38	17-18 Sep 2015	Washington, DC		INCITS
39	27 Oct 2015	Teleconference		ISO
40	23 Nov 2015	Teleconference		ISO
41	11-12 Jan 2016	Orlando, FL, USA		US NB
42	8 Feb 2016	Teleconference		ISO
43	7 Mar 2016	Teleconference	6	ISO
44	15-16 Apr 2016	London, UK	6	BSI
45	14-15 Jun 2016	Pisa, Italy	6	
46	15-16 Sep 2016	Vienna, Austria	13	
47	23-24 Jan 2017	Orlando, FL	9	
48	6-7 April 2017	Toronto, Canada	12	
49	19-20 June 2017	Vienna, Austria	8	
50	16-17 Aug 2017	London UK		
51	6-8 Nov 2017	Albuquerque NM		
52	22-23 Jan 2018	Phoenix AZ	6	
53	26-27 Apr 2018	Brno Czech Republic	6	
54	14 May 2018	WebEx	3	

4.5. FUTURE MEETINGS

#55 Rapperswil, Switzerland	6-8 June 2018 (with WG 21)
#56 Telemeeting	16 July 2018
#57 Toronto, ON Canada	12-14 Sep 2018
#58 San Diego, CA	8-9 Nov 2018 (with WG 21)
#59 Phoeniz AZ	21-22 June 2019
#60 Telemeeting	TBD March 2019
#61 (with WG 21)	TBD April 2019
#62 Telemeeting	TBD May 2019
#63 Cologne Germany	TBD Jume 2019
#64 Seoul, South Korea	22-23 Aug 2019
#65 Belfast, Northern Ireland	TBD Oct 2019 (with WG 21)

WG 23 conducts intermeeting telemeetings in conjunction with the four face-to-face meetings annually, which are pre-meeting teleconferences to organize material for the in-person meetings.