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/N0718

Date: 2016-06-12

PERIOD COVERED: July 2016 – June 2017

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

JTC 1 17960, *Code Signing for Source Code.* This project is to produce an International Standard, and has been published.

1.2.2. PROJECTS UNDERWAY

JTC 1 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.

JTC 1 24772-2, *Guidance to Avoiding Vulnerabilities in Programming Languages – Part 2, Vulnerability descriptions for programming language Ada.* This is the update of TR24772:2013 Annex C for language specific vulnerabilities for Ada, following the project split of project 22.24772.

JTC 1 24772-2, *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.

JTC 1 24772-2, *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.

JTC 1 24772-2, *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.

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, after splitting the project and the TR into Part 1, language independent part, and Parts 2 through 8 for language-specific vulnerability descriptions for Ada, C, Python, and Fortran.

2.3. RESOURCES

Seven national bodies have participated in the WG 23 meetings this year: Canada, China, Italy, Japan, Korea, 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 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 |  | 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 |  | No Liaison |
| SC 27/WG 3 |  | Security evaluation, testing and specification |  | Stephen Michell |
| ECMA TC39/TG2 |  | C# |  | No liaison, terminate |
| JSR-282/JSR-302 |  | Real-Time/Safety-Critical-Java |  | No Liaison, terminate |
| 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 24772-2, *Guidance to Avoiding Vulnerabilities in Programming Languages – Part 3, Vulnerability descriptions for programming language C.*

JTC 1 24772-2, *Guidance to Avoiding Vulnerabilities in Programming Languages – Part 4, Vulnerability descriptions for programming language Python.*

JTC 1 24772-2, *Guidance to Avoiding Vulnerabilities in Programming Languages – Part 8, Vulnerability descriptions for programming language Fortran.*

At that point, 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

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

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 arose during the next year.

3.5.  WORK PROGRAM PRIORITIES

See 4.1.

**4. OTHER ITEMS**

4.1. POSSIBLE ACTION REQUESTS AT FORTHCOMING 2016 PLENARY

WG 23 requests the the following Liaisons be terminated:

|  |
| --- |
| ECMA TC39/TG2 |
| JSR-282/JSR-302 |
| Linux Foundation |
| MDC |

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 | Number attendees | Host |
| 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 |
| 37 | 3 Aug 2015 | Teleconference |  | ISO |
| 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 |  |  |

4.5. FUTURE MEETINGS

#50 London, UK 17-18 August 2017

#51 Sandia, NM 6-8 Nov 2017

#52 Phoeniz, NM 22-23 Jan 2018

#53 Chez Republic TBD Apr 2018

#54 TBD Europe TBD June 2018

#55 Toronto, Canada 13-14 Sep 2018

WG 23 is still conducting monthly teleconferences in conjunction with the four face-to-face meetings annually, and are treating the teleconferences as pre-meeting teleconferences to organize material for the meetings.