ISO/IEC JTC 1/SC 22/WG 23 N 0445

Guidelines for Publicity

David Keaton

2013-03-14

Now that the second edition of TR 24772 has been published, it is a good time to put some extra effort into publicity. I expect my national body to ask me what we have done and what they should say to the media about it. I would like to establish some guidelines for myself, so that I stay on message and convey the correct information that WG 23 intends. Other people might like to refer to such guidelines for similar reasons.

I have listed some questions and answers below to help with this.

What is TR 24772?

ISO/IEC TR 24772 is a technical report providing guidance to avoiding vulnerabilities that occur in programming languages.

What is a vulnerability?

In this context, a vulnerability is any weakness that can be exploited or triggered by a hacker or other threat.

Who is the audience?

The technical report is intended to be a resource for software developers regarding vulnerabilities that may occur in their programming language of choice, so they can adapt their software and anticipate future vulnerabilities before they make it into production software. In addition, it can be used to help project managers select the programming language that best fits their problem domain. It also provides guidance to participants in programming language standardization efforts, to avoid vulnerabilities in future programming language design.

How does this fit in with other current efforts?

TR 24772 (Edition 2 published, WG 23)

ISO/IEC TR 24772 provides guidance across a spectrum of programming languages, for software developers and programming language designers. The focus is on vulnerabilities that arise due to the design of programming languages or their run-time environments.

TS 17961 (in draft stage, WG 14)

ISO/IEC TS 17961 is a technical specification providing secure coding rules for the C programming language, for use in developing automatic analysis tools to catch potential security problems in C programs.

CERT C Secure Coding Standard (published, CERT [non-ISO])

The CERT C Secure Coding Standard provides software developers with guidance for avoiding application vulnerabilities, specifically tailored to software being developed in the C programming language for security-related applications. The focus is on guidelines that the software developer can follow while creating or maintaining software.

MISRA C (published, MISRA [non-ISO])

MISRA C is a set of coding rules initially developed by the automotive industry for avoiding vulnerabilities in the development of C programs for use in embedded safety-related applications. Subsequently it has been adopted in other safety-critical embedded domains, such as aerospace.

Safety-Critical Java (published, Open Group [non-ISO])

Safety-Critical Java defines the capabilities needed to use Java for safety-critical applications.

Programming Language Standards

In addition, two ISO programming language standards have recently published revisions that include new language and library features for use in environments where security or safety are important. They are Ada (ISO/IEC 8652:2012), and C (ISO/IEC 9899:2011).

What is new in Edition 2 of TR 24772?

ISO/IEC TR 24772:2013 (the second edition) has added guidance for new vulnerabilities and refined the guidance for some existing ones. It has also added annexes providing detailed coverage of the following programming languages: Ada, C, Python, Ruby, SPARK, and PHP.