Guidelines for Publicity

David Keaton

2013-03-13

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 below, along with my preliminary attempts at answering them. I would appreciate it if the committee would correct me where necessary.

What is TR 24772?

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

Who is the audience?

The technical report is intended to be a resource for software developers regarding vulnerabilities that may occur in their language of choice, so they can adapt their software and anticipate future vulnerabilities before they make it into production software. 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 languages, for software developers and language designers. The focus is on vulnerabilities that arise due to the design of 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])

[I include this only because people will ask whether we overlap with it, since it has a mission that is related to ours.]

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. The focus is on guidelines that the software developer can follow while creating or maintaining software.

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

[Origins in the automotive industry; other people are better qualified than me to expand on this. I know it has a unique place in this set of efforts. What is the best way to describe it?]

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 languages: Ada, C, Python, Ruby, SPARK, and PHP.