TECHNICAL REPORT

ISO/IEC TR 24731-1

First edition
2007-09-01

Information technology — Programming languages, their environments and system software interfaces — Extensions to the C library

Part 1: Bounds-checking interfaces

Technologies de l'information — Langages de programmation, leurs environnements et leurs systèmes d'interface de logiciel — Extensions à la bibliothèque C —

Partie 1: Interfaces des contrôles des bornes

Reference number
ISO/IEC TR 24731-1:2007(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 24731-1, which is a Technical Report of type 2, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 22, *Programming languages, their environments and system software interfaces*.

ISO/IEC 24731 consists of the following part, under the general title *Information technology — Programming languages, their environments and system software interfaces — Extensions to the C library*:

— *Part 1: Bounds-checking interfaces* [Technical Report]

Introduction

Traditionally, the C library has contained many functions that trust the programmer to provide output character arrays big enough to hold the result being produced. Not only do these functions not check that the arrays are big enough, they frequently lack the information needed to perform such checks. While it is possible to write safe, robust, and error-free code using the existing library, the library tends to promote programming styles that lead to mysterious failures if a result is too big for the provided array.

A common programming style is to declare character arrays large enough to handle most practical cases. However, if these arrays are not large enough to handle the resulting strings, data can be written past the end of the array overwriting other data and program structures. The program never gets any indication that a problem exists, and so never has a chance to recover or to fail gracefully.

Worse, this style of programming has compromised the security of computers and networks. Buffer overflows can often be exploited to run arbitrary code with the permissions of the vulnerable (defective) program.

If the programmer writes runtime checks to verify lengths before calling library functions, then those runtime checks frequently duplicate work done inside the library functions, which discover string lengths as a side effect of doing their job.

This Technical Report provides alternative functions for the C library that promote safer, more secure programming. The functions verify that output buffers are large enough for the intended result and return a failure indicator if they are not. Data is never written past the end of an array. All string results are null terminated.

This Technical Report also addresses another problem that complicates writing robust code: functions that are not re-entrant because they return pointers to static objects owned by the function. Such functions can be troublesome since a previously returned result can change if the function is called again, perhaps by another thread.

Information technology — Programming languages, their environments and system software interfaces — Extensions to the C library —

Part 1: Bounds-checking interfaces

1. Scope

This Technical Report specifies a series of extensions of the programming language C, specified by International Standard ISO/IEC 9899:1999. These extensions can be useful in the mitigation of security vulnerabilities in programs, and consist of a new predefined macro, and new functions, macros, and types declared or defined in existing standard headers.

International Standard ISO/IEC 9899:1999 provides important context and specification for this Technical Report. Clauses 3 and 4 of this Technical Report are to be read as if they were merged into Clauses 3 and 4 of ISO/IEC 9899:1999. Clause 5 of this Technical Report is to be read as if it were merged into Subclause 6.10.8 of ISO/IEC 9899:1999. Clause 6 of this Technical Report is to be read as if it were merged into the parallel structure of named Subclauses of Clause 7 of ISO/IEC 9899:1999. Statements made in ISO/IEC 9899:1999, whether about the language or library, apply to this Technical Report unless a corresponding section of this Technical Report states otherwise. In particular, Subclause 7.1.4 ("Use of library functions") of ISO/IEC 9899:1999 applies to this Technical Report.

2. Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9899:1999, *Programming languages — C*

ISO/IEC 9899:1999/Cor.1:2001, *Programming languages — C — Technical Corrigendum 1*

ISO/IEC 9899:1999/Cor.2:2004, *Programming languages — C — Technical Corrigendum 2*

ISO 31−11:1992, *Quantities and units — Part 11: Mathematical signs and symbols for use in the physical sciences and technology*

ISO/IEC 2382−1:1993, *Information technology — Vocabulary — Part 1: Fundamental terms*

