Coverity Support for ISO/IEC TS 17961

Fully ensure the safety, reliability, and security of software written in C

Overview

The technical specification ISO/IEC TS 17961 is a set of well-documented and well-enforced coding rules for the C programming language. It is an important milestone in introducing best practices for ensuring the safety, reliability, security, and integrity of software written in C. Notably, the specification is designed to be enforceable by software code analyzers using static analysis techniques. This greatly reduces the cost of compliance by way of automation.

Adhering to coding standards is a crucial step in establishing best coding practices. Standards adherence is particularly important in safety-critical, high-impact industries, such as automotive, medical, and networking. Software defects in products coming from these industries manifest themselves physically and tangibly—often with life-threatening consequences.

Black Duck provides a comprehensive solution that checks for all secure coding rules specified in the ISO/IEC TS 17961 standard.

ISO/IEC TS 17961

ISO/IEC TS 17961 is defined by two publications from the International Organization for Standardization:

- ISO/IEC TS 17961:2013: Information technology—Programming languages, their environments and system software interfaces—C secure coding rules (https://www.iso.org/standard/61134.html)
- ISO/IEC TS 17961:2013/Cor 1:2016: Information technology—Programming languages, their environments and system software interfaces—C secure coding rules, Technical Corrigendum 1 (https://www.iso.org/standard/72086.html)

The technical specification defines secure coding rules for C. These rules are designed to provide a check against programming flaws that lead to vulnerabilities, regardless of whether the code is deployed in a security-critical environment.

The specification is focused on security vulnerabilities. Some rules pertain to data taint analysis: tracing data propagation from sources to sinks. Tainted data should be sanitized before being used. Coverity® Static Analysis by Black Duck, with its state-of-the-art dataflow analysis techniques, can accurately identify such vulnerabilities in source code.

Technical Specifications

Rule	Name	Supported
5.1	ptrcomp	Yes
5.2	accfree	Yes
5.3	accsig	Yes
5.4	boolasgn	Yes
5.5	asyncsig	Yes
5.6	argcomp	Yes
5.7	sigcall	Yes
5.8	syscall	Yes
5.9	padcomp	Yes
5.10	intptrconv	Yes
5.11	alignconv	Yes
5.12	filecpy	Yes
5.13	funcdecl	Yes
5.14	nullref	Yes
5.15	addrescape	Yes
5.16	signconv	Yes

Rule	Name	Supported
5.17	swtchdflt	Yes
5.18	fileclose	Yes
5.19	liberr	Yes
5.20	libptr	Yes
5.21	insufmem	Yes
5.22	invptr	Yes
5.23	dblfree	Yes
5.24	usrfmt	Yes
5.25	inverrno	Yes
5.26	diverr	Yes
5.27	ioileave	Yes
5.28	strmod	Yes
5.29	libmod	Yes
5.30	intoflow	Yes
5.31	nonnullcs	Yes
5.32	chrsgnext	Yes

Rule	Name	Supported
5.33	restrict	Yes
5.34	xfree	Yes
5.35	uninitref	Yes
5.36	ptrobj	Yes
5.37	taintstrcpy	Yes
5.38	sizeofptr	Yes
5.39	taintnoproto	Yes
5.40	taintformatio	Yes
5.41	xfilepos	Yes
5.42	libuse	Yes
5.43	chreof	Yes
5.44	resident	Yes
5.45	invfmtstr	Yes
5.46	taintsink	Yes

**ISO (International Organization for Standardization) holds the copyright to the rules listed in this table, and all other rights to the rules are reserved by ISO*

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.