
# List of Weaknesses Included in the Automated Source Code Data Protection Measure

October 2020

## Overview of Structural Quality Measurement in Software

Measurement of the structural quality characteristics of software has a long history in software engineering. These characteristics are also referred to as the structural, internal, technical, or engineering characteristics of software source code. Software quality characteristics are increasingly incorporated into development and outsourcing contracts as the equivalent of service level agreements. That is, target thresholds based on structural quality measures are being written into contracts as acceptance criteria for delivered software.

Recent advances in measuring the structural quality of software involve detecting violations of good architectural and coding practice from statically analyzing source code. Good architectural and coding practices can be stated as rules for engineering software products. Violations of these rules will be called weaknesses to be consistent with terms used in the Common Weakness Enumeration which lists the weaknesses used in this measure.

The Automated Source Code Quality Measures from CISQ are calculated from counts of what industry experts have determined to be most severe weaknesses. Consequently, they provide strong indicators of the quality of a software system and the probability of operational or cost problems related to each measure's domain.

The weaknesses comprising the CISQ Automated Source Code Data Protection Measure are grouped by measure in the table. The Common Weakness Enumeration repository (an ITU standard) has recently been expanded to include weaknesses from quality characteristics beyond security. All weaknesses included in this measure are identified by their CWE number from the repository. The title and description of CWEs is taken from information in the online CWE repository (cwe.mitre.org). Each weakness will be described as a 'quality measure element' to remain consistent with the structure of software quality measures enumerated in ISO/IEC 25020.

Some weaknesses drawn from the CWE repository (parent weaknesses) have related weaknesses listed as 'contributing weaknesses' ('child weaknesses' in the CWE). Contributing weaknesses represent variants of how the parent weakness can be instantiated in software. In the following table the cells containing CWE IDs for parents are presented in a darker blue than the cells containing contributing weaknesses. Based on their severity, not all children were included in this standard. Compliance to the CISQ measures is assessed at the level of the parent weakness. A technology must be able to detect at least one of the contributing weaknesses to be assessed compliant on the parent weakness.

## Automated Source Code Data Protection Measure Element Descriptions

The quality measure elements (weaknesses violating software quality rules) that compose the CISQ Automated Source Code Data Protection Measure are presented in Table 1. This measure contains 36 parent weaknesses and 53 contributing weaknesses.

**Table 1. Quality Measure Elements for Automated Source Code Data Protection Measure**

| CWE # | Descriptor |
|---|---|
| CWE-22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') link |
| CWE-23 | Relative Path Traversal link |
| CWE-36 | Absolute Path Traversal link |
| CWE-77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') link |
| CWE-78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') link |
| CWE-88 | Argument Injection or Modification link |
| CWE-624 | Executable Regular Expression Error link |
| CWE-917 | Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') link |
| CWE-79 | Improper Neutralization of Input During Web Page Generation ('Cross Site Scripting') link |
| CWE-89 | Improper Neutralization of Special Elements used in a SQL Command ('SQL Injection') link |
| CWE-90 | Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') link |
| CWE-91 | XML Injection (aka Blind XPath Injection) link |
| CWE-99 | Improper Control of Resource Identifiers ('Resource Injection') link |

| | |
|---|---|
| CWE-119 | Improper Restriction of Operations within the Bounds of a Memory Buffer link |
| CWE-120 | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') link |
| CWE-123 | write-what-where-condition link |
| CWE-125 | Out-of-bounds read link |
| CWE-130 | Improper Handling of Length Parameter Inconsistency link |
| CWE-786 | Access of Memory Location Before Start of Buffer link |
| CWE-787 | Out-of-bounds Write link |
| CWE-788 | Access of Memory Location After End of Buffer link |
| CWE-805 | Buffer Access with Incorrect Length Value link |
| CWE-822 | Untrusted Pointer Dereference link |
| CWE-823 | Use of Out-of-range Pointer Offset link |
| CWE-824 | Access of Uninitialized Pointer link |
| CWE-825 | Expired Pointer Dereference link |
| CWE-129 | Improper Validation of Array Index link |
| CWE-134 | Use of Externally Controlled Format String link |

| | |
|---|---|
| CWE-170 | Improper Null Termination link |
| CWE-213 | Exposure of Sensitive Information Due to Incompatible Policies link |
| CWE-284 | Improper Access Control link |
| CWE-285 | Improper Authorization link |
| CWE-287 | Improper Authentication link |
| CWE-288 | Authentication Bypass Using an Alternate Path or Channel link |
| CWE-639 | Authorization Bypass Through User-Controlled Key link |
| CWE-862 | Missing Authorization link |
| CWE-863 | Incorrect Authorization link |
| CWE-311 | Missing Encryption of Sensitive Data link |
| CWE-359 | Exposure of Private Personal Information to an Unauthorized Actor link |
| CWE-404 | Improper Resource Shutdown or Release link |
| CWE-761 | Free of Pointer not at Start of Buffer link |
| CWE-762 | Mismatched Memory Management Routines link |
| CWE-763 | Release of Invalid Pointer or Reference link |

| | |
|---|---|
| CWE-772 | Missing Release of Resource after Effective Lifetime link |
| CWE-775 | Missing Release of File Descriptor or Handle after Effective Lifetime link |
| CWE-424 | Improper Protection of Alternate Path link |
| CWE-434 | Unrestricted Upload of File with Dangerous Type link |
| CWE-502 | Deserialization of Untrusted Data link |
| CWE-562 | Return of Stack Variable Address link |
| CWE-606 | Unchecked Input for Loop Condition |
| CWE-611 | Improper Restriction of XML External Entity Reference ('XXE') link |
| CWE-643 | Improper Neutralization of Data within XPath Expressions ('XPath Injection') link |
| CWE-652 | Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') link |
| CWE-662 | Improper Synchronization link |
| CWE-667 | Improper Locking link |
| CWE-764 | Multiple Locks of a Critical Resource link |
| CWE-820 | Missing Synchronization link |
| CWE-821 | Incorrect Synchronization link |

| | |
|---|---|
| CWE-1058 | Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element link |
| CWE-1096 | Singleton Class Instance Creation without Proper Locking or Synchronization link |
| CWE-366 | Race Condition within a Thread link |
| CWE-543 | Use of Singleton Pattern Without Synchronization in a Multithreaded Context link |
| CWE-567 | Unsynchronized Access to Shared Data in a Multithreaded Context link |
| CWE-665 | Improper Initialization link |
| CWE-456 | Missing Initialization of a Variable link |
| CWE-457 | Use of Uninitialized Variable link |
| CWE-672 | Operation on a Resource after Expiration or Release link |
| CWE-415 | Double Free link |
| CWE-416 | Use After Free link |
| CWE-681 | Incorrect Conversion between Numeric Types link |
| CWE-194 | Unexpected Sign Extension link |
| CWE-195 | Signed to Unsigned Conversion Error link |
| CWE-196 | Unsigned to Signed Conversion Error link |

| | |
|---|---|
| CWE-197 | Numeric Truncation Error link |
| CWE-682 | Incorrect Calculation link |
| CWE-131 | Incorrect Calculation of Buffer Size link |
| CWE-369 | Divide by Zero link |
| CWE-703 | Improper Check or Handling of Exceptional Conditions link |
| CWE-248 | Uncaught Exception link |
| CWE-391 | Unchecked Error Condition link |
| CWE-392 | Missing Report of Error Condition link |
| CWE-704 | Incorrect Type Conversion or Cast link |
| CWE-732 | Incorrect Permission Assignment for Critical Resource link |
| CWE-798 | Use of Hard-coded Credentials link |
| CWE-259 | Use of Hard-coded Password link |
| CWE-321 | Use of Hard-coded Cryptographic Key link |
| CWE-908 | Use of Uninitialized Resource link |
| CWE-915 | Improperly Controlled Modification of Dynamically-Determined Object Attributes link |

| CWE-1051 | Initialization with Hard-Coded Network Resource Configuration Data link |
|---|---|