

CWE WEAKNESS IDS MAPPED TO CODESONAR® 6.2 JAVA WARNING CLASSES

TRUSTED LEADERS OF SOFTWARE ASSURANCE AND ADVANCED CYBER-SECURITY SOLUTIONS

WWW.GRAMMATECH.COM

INTRODUCTION

The Common Weakness Enumeration (CWE™) is a list of software weakness types. Creating the list is a community initiative aimed at creating specific and succinct definitions for each common weakness type.

Every CodeSonar warning report includes the numbers of any CWE weakness IDs that are closely mapped to the warning's class. (The close mapping for a warning class is the set of categories—including CWE weakness IDs—that most closely match the class, if any).

You can configure CodeSonar to enable and disable warning classes mapped to specific CWE weakness IDs, or use build presets to enable all warning classes that are closely mapped to any CWE weakness IDs. In addition, you can use the CodeSonar search function to find warnings related to specific CWE weakness IDs.

CodeSonar 6.2 uses CWE v4.4 (released March 15, 2021).

For more information on Common Weakness Enumeration:

<https://cwe.mitre.org/data/index.html>

The remainder of this document comprises two tables:

- A table showing the close mapping between CodeSonar Java warning classes and CWE weakness IDs.
- A table showing the broad mapping between CodeSonar Java warning classes and CWE weakness IDs. The broad CWE mapping for a CodeSonar warning class combines CWE weakness IDs from four sources:
 1. The close CWE mapping for the class.
 2. Other CWE weakness IDs that are related to the class in a meaningful way, but not eligible for the close mapping.
 3. For all CWE weakness IDs from sources 1 and 2, all *ancestors* in the CWE hierarchy.
 4. For all CWE weakness IDs from sources 1 and 2, all *descendants* in the CWE hierarchy.

A separate document, CWE Weakness IDs Mapped to CodeSonar® C/C++ Warning Classes, lists the CodeSonar C/C++ warning classes that are closely and broadly mapped to CWE weakness IDs.

GammaTech is a leading global provider of application testing (AST) solutions used by the world's most security conscious organizations to detect, measure, analyze and resolve vulnerabilities for software they develop or use. The company is also a trusted cybersecurity and artificial intelligence research partner for the nation's civil, defense, and intelligence agencies.

CodeSonar and CodeSentry are registered trademarks of GammaTech, Inc.
© GammaTech, Inc. All rights reserved.



CWE CLOSE MAPPING: JAVA (CODESONAR V6.2P0)

The following table lists the CodeSonar Java warning classes that are closely mapped to CWEweakness IDs.

Category ID	Category Name	CodeSonar Class Name
CWE:20	Improper Input Validation	Disabled Input Validation (Java)
CWE:22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Tainted Path (Java)
CWE:74	Improper Neutralization of Special Elements in Output Used by a DownstreamComponent ('Injection')	Missing isValidFragment Override (Java) Android URL Injection (Java) DOS Injection (Java) Tainted Network Address (Java) Tainted Control (Java) Tainted Hardware Device Property (Java) Tainted Resource (Java) Tainted @Trusted Value (Java) Tainted URL (Java) Tainted Data in Vulnerable Method (Java) DLL Injection (Java) Tainted XAML (Java) Tainted XML (Java)
CWE:78	Improper Neutralization of Special Elements used in an OS Command ('OS Com-mand Injection')	Command Injection (Java)
CWE:79	Improper Neutralization of Input During Web Page Generation ('Cross-site Script-ing')	Cross Site Scripting (Java)
CWE:89	Improper Neutralization of Special Elements used in an SQL Command ('SQLInjection')	SQL Injection (Java)
CWE:90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAPInjection')	Tainted LDAP Attribute (Java)
CWE:94	Improper Control of Generation of Code ('Code Injection')	Code Injection (Java)
CWE:95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injec-tion')	Tainted Expression Evaluation (Java)
CWE:113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP ResponseSplitting')	Tainted HTTP Response (Java)
CWE:114	Process Control	DLL Injection (Java)
CWE:117	Improper Output Neutralization for Logs	Tainted Log (Java)
CWE:190	Integer Overflow or Wraparound	Cast: int Computation to long (Java)
CWE:192	Integer Coercion Error	Cast: Integer to Floating Point (Java)
CWE:197	Numeric Truncation Error	Approximate e Constant (Java) Approximate pi Constant (Java)
CWE:200	Exposure of Sensitive Information to an Unauthorized Actor	Use of Hardware ID (Java)



CWE:227	7PK - API Abuse	Ambiguous Call from Inner Class (Java) Inefficient Box-Unbox (Java) Inappropriate Instanceof (Java) Unnecessary Instantiation for GetClass (Java) compareTo in Non-Comparable Class (Java) Non-Object compareTo Parameter (Java) Array Parameter Empty (Java) Ignored Return Value for Pure Function (Java) Redundant Call for Integral Argument (Java) Shadowed Identifier (Java) equals Parameter Should Be Object (Java) Method Should Not Return null (Java)
CWE:252	Unchecked Return Value	Ignored Return Value (Java) Call Might Return Null (Java)
CWE:253	Incorrect Check of Function Return Value	Useless null Test of Return Value (Java) Null Pointer Dereference (Java)
CWE:259	Use of Hard-coded Password	Hardcoded Password (Java) Sensitive Data Written to External Storage (Java)
CWE:287	Improper Authentication	Hostname in Condition (Java) Insecure verifier Override for Hostname (Java) Use of Insecure verify for Hostname (Java) Anonymous LDAP Authentication (Java) Ineffective Cleansing of Fragment Taint (Java) LDAP Authentication Disabled (Java) Missing Authentication Annotation (Java)
CWE:295	Improper Certificate Validation	Insecure verify Override for Certificate (Java) Use of Insecure verify for Certificate (Java) Insecure Socket Factory (Java) Untrusted Network Host (Java)
CWE:319	Cleartext Transmission of Sensitive Information	Android Message Injection (Java) Tainted Message (Java)
CWE:326	Inadequate Encryption Strength	Insecure Key Derivation (Java)
CWE:327	Use of a Broken or Risky Cryptographic Algorithm	Unsafe Base64 Encoding (Java) Risky Cryptographic Algorithm (Java) Risky Cipher Field (Java) Risky Cryptographic Field (Java) Cryptographic Algorithm with Risky Default Cipher (Java) Cryptographic Algorithm with Weak Cipher (Java) Cryptographic Algorithm with Weak Hash (Java) Deprecated Cryptography Provider (Java) Risky Cipher Algorithm (Java)
CWE:328	Reversible One-Way Hash	Weak Hash Algorithm (Java) Weak Hash Algorithm Field (Java)

CWE:330	Use of Insufficiently Random Values	Hardcoded Random Seed (Java) Insecure Random Number Generator (Java)
CWE:338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	Weak Cryptographic Value (Java)
CWE:349	Acceptance of Extraneous Untrusted Data With Trusted Data	Potential LDAP Poisoning (Java) Tainted Data in Vulnerable Method (Java)
CWE:390	Detection of Error Condition Without Action	Empty Exception Handler (Java)
CWE:395	Use of NullPointerException Catch to Detect NULL Pointer Dereference	Inappropriate Exception Handler (Java)
CWE:396	Declaration of Catch for Generic Exception	Generic Exception Handler (Java)
CWE:397	Declaration of Throws for Generic Exception	Broad Throws Clause (Java)
CWE:398	7PK - Code Quality	Useless Class Cast (Java) Redundant Implements Clause (Java) Static Field Assigned Non-Static (Java) Useless null Test (Java) Useless null Test of Field (Java) Useless null Test of Parameter (Java) Redundant Call for String Argument (Java) Empty Branch Statement (Java) Unused Class (Java) Unused Field (Java)
CWE:400	Uncontrolled Resource Consumption	Closeable Not Stored (Java) Inefficient Instantiation (Java)
CWE:412	Unrestricted Externally Accessible Lock	Synchronization on Interned String (Java)
CWE:413	Improper Resource Locking	Impossible Client Side Locking (Java) Synchronization on static (Java)
CWE:440	Expected Behavior Violation	toString on Array (Java)
CWE:456	Missing Initialization of a Variable	Null Pointer Dereference (Java) Field Never Written (Java) Lambda Parameter may be null (Java)
CWE:470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	Fragment Injection (Java) Reflection Injection (Java)
CWE:476	NULL Pointer Dereference	Null Pointer Dereference (deep) (Java) Field Element may be null (deep) (Java) Field may be null (deep) (Java) null Passed to Method (deep) (Java) Actual Parameter Element may be null (Java) Return Value may Contain null Element (Java) Return Value may be null (Java) Null Pointer Dereference (Java) Null Parameter Dereference (Java) Return null Array (Java) Return null Boolean (Java) Return null Optional (Java) Unchecked Parameter Dereference (deep) (Java) Unchecked Parameter Dereference (Java) Unchecked Parameter Element Dereference (deep) (Java)

CWE:477	Use of Obsolete Function	Debug Call (Java) Debug Warning (Java)
CWE:480	Use of Incorrect Operator	Should Use == Instead of equals() (Java) Bitwise AND on Boolean Constant (Java) Inefficient Bitwise AND (Java) Bitwise OR on Boolean Constant (Java) Inefficient Bitwise OR (Java)
CWE:481	Assigning instead of Comparing	Assignment in Conditional (Java)
CWE:485	7PK - Encapsulation	Method Should be final (Java) Field Too Visible (Java) Method Should be private (Java) Static Field Too Visible (Java) Shadowed Identifier (Java)
CWE:489	Active Debug Code	Class Enables Debug Features (Java) Debug Call (Java) Method Enables Debug Features (Java)
CWE:491	Public cloneable() Method Without Final ('Object Hijack')	clone Non-cloneable (Java) clone not final (Java) clone Subclass of Non-clonable (Java)
CWE:492	Use of Inner Class Containing Sensitive Data	Inner Class Should be Static (Java)
CWE:501	Trust Boundary Violation	Tainted Bundle (Java) Tainted Session (Java)
CWE:502	Deserialization of Untrusted Data	Serialization Not Disabled (Java)
CWE:522	Insufficiently Protected Credentials	Password in Property File (Java)
CWE:524	Use of Cache Containing Sensitive Information	Sensitive Data Cached (Java)
CWE:538	Insertion of Sensitive Information into Externally-Accessible File or Directory	Sensitive Data Written to Local File (Java)
CWE:547	Use of Hard-coded, Security-relevant Constants	Hardcoded Filename (Java) Hardcoded IP Address (Java)
CWE:550	Server-generated Error Message Containing Sensitive Information	Server-generated Error Message Containing Sensitive Information
CWE:561	Dead Code	Unreachable Instruction (Java) Unused Class (Java) Unused Method (Java)
CWE:563	Assignment to Variable without Use	Unnecessary Field (Java) Unused Value: Actual Parameter (Java) Unused Value: Write to Parameter (Java) Unused Value: Variable (Java)
CWE:567	Unsynchronized Access to Shared Data in a Multithreaded Context	Missing synchronized Statement (Java) Unguarded Field (Java) Unguarded Parameter (Java) Useless volatile Modifier (Java)

CWE:570	Expression is Always False	Instanceof Always False (Java) Instanceof Always True (Java) Redundant Condition (Java) Impossible reference comparison (Java) Instanceof Always False (Java) Redundant Condition (Java) equals Always Fails (Java)
CWE:571	Expression is Always True	Instanceof Always True (Java) Redundant Condition (Java)
CWE:572	Call to Thread run() instead of start()	Synchronous Call to Thread Body (Java)
CWE:573	Improper Following of Specification by Caller	Missing Call to super (Java)
CWE:581	Object Model Violation: Just One of Equals and Hashcode Defined	Defines equals but not hashCode (Java) Defines hashCode but not equals (Java)
CWE:585	Empty Synchronized Block	Useless Synchronization (Java)
CWE:595	Comparison of Object References Instead of Object Contents	Should Use equals() Instead of == (Java) equals on Array (Java) == Always Fails (Java)
CWE:596	DEPRECATED: Incorrect Semantic Object Comparison	== Always Fails Because Types Always Different (Java)
CWE:597	Use of Wrong Operator in String Comparison	Comparison to Empty String (Java)
CWE:601	URL Redirection to Untrusted Site ('Open Redirect')	Android URL Injection (Java) Tainted URL (Java)
CWE:607	Public Static Final Field References Mutable Object	Mutable Constant Field (Java) Mutable Enumeration (Java)
CWE:609	Double-Checked Locking	Double-Checked Locking (Java)
CWE:611	Improper Restriction of XML External Entity Reference	Possible XML External Entity Reference (Java) Insecure XSLT Execution (Java)
CWE:614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	Insecure Cookie (Java)
CWE:624	Executable Regular Expression Error	Tainted Regular Expression (Java)
CWE:628	Function Call with Incorrectly Specified Arguments	Method Names Differ Only in Case (Java)
CWE:643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')	Tainted Xpath (Java)
CWE:662	Improper Synchronization	Useless volatile Modifier (Java)
CWE:664	Improper Control of a Resource Through its Lifetime	Android Leak (Java)
CWE:665	Improper Initialization	Assertion Contains Side Effects (Java) Useless Assignment (Java) Useless Assignment to Default (Java)
CWE:674	Uncontrolled Recursion	Potential Infinite Recursion (Java)
CWE:676	Use of Potentially Dangerous Function	Method Disables Security Setting (Java)
CWE:682	Incorrect Calculation	Abs on random (Java)
CWE:686	Function Call With Incorrect Argument Type	Non-overriding Method Signature (Java)
CWE:697	Incorrect Comparison	Asymmetric compareTo (Java) compareTo without equals (Java) compareTo/equals mismatch (Java)

CWE:704	Incorrect Type Conversion or Cast	Risky Class Cast (Java) Risky array store (Java)
CWE:710	Improper Adherence to Coding Standards	Naming Style Violation (Java)
CWE:732	Incorrect Permission Assignment for Critical Resource	Permissive File Mode (Java) Accessing File in Permissive Mode (Java)
CWE:749	Exposed Dangerous Method or Function	JavaScript File Access from File URLs (Java) JavaScript Enabled (Java) Missing JavaScript Execution (Java) Missing JavaScript Entry Point (Java) Risky JavaScript Interface (Java) Universal JavaScript Access to File URLs (Java)
CWE:757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')	Deprecated Transfer Protocol (Java)
CWE:768	Incorrect Short Circuit Evaluation	Bitwise AND on Boolean (Java) Bitwise OR on Boolean (Java)
CWE:771	Missing Reference to Active Allocated Resource	Unused Object (Java)
CWE:772	Missing Release of Resource after Effective Lifetime	Closeable Not Closed (Java)
CWE:820	Missing Synchronization	Unguarded Method (Java)
CWE:833	Deadlock	Blocking in Critical Section (Java) Tainted LDAP Filter (Java)
CWE:909	Missing Initialization of Resource	Empty jar File Archived (Java) Empty zip File Archived (Java)
CWE:913	Improper Control of Dynamically-Managed Code Resources	Insecure Class Loader (Java) Deserializable Class (Java) Deserializing Non-Serializable Class (Java) Nonserializable Field Element (Java) Nonserializable Field (Java) Nonserializable Outer Class (Java) Missing Serial Version Field (Java) Unexpected Serial Version Field (Java)
CWE:915	Improperly Controlled Modification of Dynamically-Determined Object Attributes	Reflection Bypasses Member Accessibility (Java) Reflection Modifies Member Accessibility (Java)
CWE:916	Use of Password Hash With Insufficient Computational Effort	Weak Cryptographic Value (Java) Inadequate Salt (Java)
CWE:922	Insecure Storage of Sensitive Information	Certificate Added to Root Store (Java)
CWE:1023	Incomplete Comparison with Missing Factors	Missing Equals Override (Java)
CWE:1077	Floating Point Comparison with Incorrect Operator	Floating Point Equality (Java)
CWE:1126	Declaration of Variable with Unnecessarily Wide Scope	Unnecessary Field (Java)
CWE:1164	Irrelevant Code	Unused Object (Java) Field Never Read (Java)
CWE:1173	Improper Use of Validation Framework	Missing isValidFragment Override (Java)
CWE:1176	Inefficient CPU Computation	Single-use Random Number Generator (Java)



CWE IDS THAT ARE BROADLY MAPPED TO ONE OR MORE CODESONAR JAVA WARNINGCLASSES (CODESONAR V6.2P0)

The following table lists the CWE IDs that are broadly mapped to one or more CodeSonar Java warning classes.

CWE:19	CWE:310	CWE:492	CWE:671	CWE:736	CWE:820	CWE:887	CWE:958
CWE:20	CWE:311	CWE:501	CWE:674	CWE:737	CWE:821	CWE:888	CWE:959
CWE:22	CWE:319	CWE:502	CWE:676	CWE:738	CWE:833	CWE:889	CWE:960
CWE:73	CWE:326	CWE:522	CWE:681	CWE:739	CWE:844	CWE:890	CWE:961
CWE:74	CWE:327	CWE:524	CWE:682	CWE:740	CWE:845	CWE:892	CWE:962
CWE:77	CWE:328	CWE:538	CWE:684	CWE:741	CWE:846	CWE:893	CWE:963
CWE:78	CWE:330	CWE:547	CWE:686	CWE:742	CWE:847	CWE:894	CWE:965
CWE:79	CWE:338	CWE:550	CWE:691	CWE:743	CWE:848	CWE:895	CWE:966
CWE:89	CWE:344	CWE:557	CWE:693	CWE:744	CWE:849	CWE:896	CWE:971
CWE:90	CWE:345	CWE:561	CWE:697	CWE:745	CWE:850	CWE:897	CWE:975
CWE:91	CWE:349	CWE:563	CWE:699	CWE:746	CWE:851	CWE:898	CWE:977
CWE:93	CWE:361	CWE:567	CWE:700	CWE:747	CWE:852	CWE:899	CWE:978
CWE:94	CWE:388	CWE:569	CWE:703	CWE:748	CWE:853	CWE:900	CWE:980
CWE:95	CWE:389	CWE:570	CWE:704	CWE:749	CWE:854	CWE:902	CWE:981
CWE:113	CWE:390	CWE:571	CWE:705	CWE:750	CWE:855	CWE:903	CWE:982
CWE:114	CWE:392	CWE:572	CWE:706	CWE:751	CWE:857	CWE:905	CWE:984
CWE:116	CWE:395	CWE:573	CWE:707	CWE:752	CWE:858	CWE:906	CWE:985
CWE:117	CWE:396	CWE:581	CWE:710	CWE:753	CWE:859	CWE:907	CWE:986
CWE:133	CWE:397	CWE:585	CWE:711	CWE:754	CWE:860	CWE:909	CWE:987
CWE:136	CWE:398	CWE:595	CWE:712	CWE:755	CWE:861	CWE:913	CWE:989
CWE:137	CWE:399	CWE:597	CWE:713	CWE:757	CWE:864	CWE:915	CWE:990
CWE:189	CWE:400	CWE:601	CWE:714	CWE:768	CWE:865	CWE:916	CWE:991
CWE:190	CWE:404	CWE:607	CWE:715	CWE:771	CWE:866	CWE:922	CWE:992
CWE:192	CWE:405	CWE:609	CWE:717	CWE:772	CWE:867	CWE:928	CWE:994
CWE:197	CWE:411	CWE:610	CWE:718	CWE:798	CWE:868	CWE:929	CWE:997
CWE:199	CWE:412	CWE:611	CWE:719	CWE:800	CWE:871	CWE:930	CWE:998
CWE:200	CWE:413	CWE:614	CWE:720	CWE:801	CWE:872	CWE:931	CWE:1000
CWE:209	CWE:438	CWE:624	CWE:721	CWE:802	CWE:873	CWE:932	CWE:1001
CWE:221	CWE:440	CWE:628	CWE:722	CWE:803	CWE:874	CWE:933	CWE:1002
CWE:227	CWE:456	CWE:629	CWE:723	CWE:808	CWE:875	CWE:934	CWE:1003
CWE:252	CWE:465	CWE:635	CWE:724	CWE:809	CWE:876	CWE:935	CWE:1005
CWE:253	CWE:470	CWE:642	CWE:725	CWE:810	CWE:877	CWE:938	CWE:1006
CWE:254	CWE:471	CWE:643	CWE:727	CWE:811	CWE:878	CWE:943	CWE:1008
CWE:255	CWE:476	CWE:657	CWE:728	CWE:812	CWE:879	CWE:944	CWE:1009
CWE:259	CWE:477	CWE:662	CWE:729	CWE:813	CWE:880	CWE:945	CWE:1010
CWE:265	CWE:480	CWE:664	CWE:730	CWE:815	CWE:882	CWE:946	CWE:1011
CWE:284	CWE:481	CWE:665	CWE:731	CWE:816	CWE:883	CWE:947	CWE:1012
CWE:285	CWE:485	CWE:667	CWE:732	CWE:817	CWE:884	CWE:949	CWE:1013
CWE:287	CWE:489	CWE:668	CWE:734	CWE:818	CWE:885	CWE:950	CWE:1014
CWE:295	CWE:491	CWE:670	CWE:735	CWE:819	CWE:886	CWE:957	CWE:1015



CWE:1016	CWE:1030	CWE:1128	CWE:1140	CWE:1152	CWE:1166	CWE:1180	CWE:1214
CWE:1019	CWE:1031	CWE:1129	CWE:1141	CWE:1154	CWE:1167	CWE:1181	CWE:1215
CWE:1020	CWE:1032	CWE:1130	CWE:1142	CWE:1157	CWE:1169	CWE:1182	CWE:1228
CWE:1023	CWE:1033	CWE:1131	CWE:1143	CWE:1158	CWE:1170	CWE:1186	CWE:1305
CWE:1024	CWE:1034	CWE:1133	CWE:1144	CWE:1159	CWE:1171	CWE:1194	CWE:1306
CWE:1025	CWE:1071	CWE:1134	CWE:1145	CWE:1161	CWE:1173	CWE:1200	CWE:1307
CWE:1026	CWE:1076	CWE:1135	CWE:1147	CWE:1162	CWE:1176	CWE:1208	CWE:1308
CWE:1027	CWE:1077	CWE:1136	CWE:1148	CWE:1163	CWE:1177	CWE:1210	CWE:1309
CWE:1028	CWE:1078	CWE:1137	CWE:1149	CWE:1164	CWE:1178	CWE:1211	CWE:1340
CWE:1029	CWE:1126	CWE:1139	CWE:1150	CWE:1165	CWE:1179	CWE:1213	CWE:1350

