# [CS] CODESECURE

# CWE WEAKNESS IDS
## MAPPED TO CODESONAR® 8.0 JAVA WARNING CLASSES

## 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 closelymapped 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 8.0 is using CWE v4.12, released June 29, 2023.

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, liststhe CodeSonar C/C++ warning classes that are closely and broadly mapped to CWE weakness IDs.

CodeSecure 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.

## CWE CLOSE MAPPING: JAVA (CODESONAR V8.10)

The following table lists the CodeSonar Java warning classes that are closely mapped to CWE weakness 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) <br> Android URL Injection (Java) <br> DOS Injection (Java) <br> Tainted Network Address (Java) <br> Tainted Control  (Java) <br> Tainted Hardware Device Property (Java) <br> Tainted Resource (Java) <br> Tainted @Trusted Value (Java) <br> Tainted URL (Java) <br> Tainted Data in Vulnerable Method (Java) <br> DLL Injection (Java) <br> Tainted XAML (Java) <br> Tainted XML (Java) |
| CWE:78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | Command Injection (Java) |
| CWE:79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | Cross Site Scripting (Java) <br> Cross Site Scripting In Error Message Web Page (Java) |
| CWE: 81 | Improper Neutralization of Script in an Error Message Web Page | Cross Site Scripting In Error Message Web Page (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 Injection') | Tainted Expression Evaluation (Java) |
| CWE:113 | Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') | Tainted HTTP Response (Java) |
| CWE:114 | Process Control | DLL Injection (Java) |
| CWE:117 | Improper Output Neutralization for Logs | Tainted Log (Java) |
| CWE:134 | Use of Externally-Controlled Format String | Format String Injection (C#) |
| 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) <br> Approximate pi Constant (Java) |
| CWE:200 | Exposure of Sensitive Information to an Unauthorized Actor | Use of Hardware ID (Java) |
| CWE:252 | Unchecked Return Value | Ignored Return Value (Java) <br> Call Might Return Null (Java) <br> Ignored Return Value for Pure Function (Java) |
| CWE:253 | Incorrect Check of Function Return Value | Useless null Test of Return Value (Java) <br> Null Pointer Dereference (Java) |
| CWE:259 | Use of Hard-coded Password | Hardcoded Password (Java) <br> 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) |
| | | Ineffective Cleansing of Fragment Taint (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:321 | Use of Hard-coded Cryptographic Key | Hardcoded Cryptographic Key (Java) |
| CWE:325 | Missing Cryptographic Step | Missing Required Cryptographic Step (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) |
| | | Deprecated Cryptography Provider (Java) |
| | | Risky Cipher Algorithm (Java) |
| CWE:328 | Use of Weak 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) |
| | | Legacy Random Generator (Java) |
| CWE:336 | Same Seed in Pseudo-Random Number Generator (PRNG) | Use of Same Seed (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:383 | J2EE Bad Practices: Direct Use of Threads | Direct Thread Usage in Http Servlet (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: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) |
| | | Method Should Not Return null (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:486 | Comparison of Classes by Name | Comparison to Class Names (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)<br>Unused Class (Java)<br>Unused Method (Java) |
| CWE:563 | Assignment to Variable without Use | Unnecessary Field (Java)<br>Unused Value: Actual Parameter (Java)<br>Unused Value: Write to Parameter (Java)<br>Unused Value: Variable (Java) |
| CWE:567 | Unsynchronized Access to Shared Data in a Multithreaded Context | Missing synchronized Statement (Java)<br>Unguarded Field (Java)<br>Unguarded Parameter (Java)<br>Useless volatile Modifier (Java) |
| CWE:570 | Expression is Always False | Instanceof Always False (Java)<br>Instanceof Always True (Java)<br>Redundant Condition (Java)<br>Impossible reference comparison (Java)<br>Instanceof Always False (Java)<br>Redundant Condition (Java)<br>equals Always Fails (Java) |
| CWE:571 | Expression is Always True | Instanceof Always True (Java)<br>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:580 | clone() Method Without super.clone() | Clone Call to Super is Missing (Java) |
| CWE:581 | Object Model Violation: Just One of Equals and Hashcode Defined | Defines equals but not hashCode (Java)<br>Defines hashCode but not equals (Java) |
| CWE:582 | "Array Declared Public, Final, and Static" | Mutable Public Static Final Array (Java) |
| CWE:585 | Empty Synchronized Block | Useless Synchronization (Java) |
| CWE:586 | Explicit Call to Finalize() | Explicit Finalize (Java) |
| CWE:595 | Comparison of Object References Instead of Object Contents | Should Use equals() Instead of == (Java)<br>equals on Array (Java)<br>== 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)<br>Tainted URL (Java)<br>Open Redirect (Java) |
| CWE:607 | Public Static Final Field References Mutable Object | Mutable Constant Field (Java)<br>Mutable Enumeration (Java)<br>Mutable Public Static Final Array (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:613 | Insufficient Session Expiration | Unsafe Session Expiration Time (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) <br> Array Parameter Empty (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) <br> Useless Assignment (Java) <br> 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) <br> compareTo without equals (Java) <br> compareTo/equals mismatch (Java) |
| CWE:698 | Execution After Redirect (EAR) | Execution After Redirect (Java) |
| CWE:704 | Incorrect Type Conversion or Cast | Risky Class Cast (Java) <br> 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) <br> Accessing File in Permissive Mode (Java) |
| CWE:749 | Exposed Dangerous Method or Function | JavaScript File Access from File URLs (Java) <br> JavaScript Enabled (Java) <br> Missing JavaScript Execution (Java) <br> Missing JavaScript Entry Point (Java) <br> Risky JavaScript Interface (Java) <br> 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) <br> 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:789 | Memory Allocation with Excessive Size Value | Tainted Allocation Size (Java) |
| CWE:820 | Missing Synchronization | Unguarded Method (Java) |
| CWE:833 | Deadlock | Blocking in Critical Section (Java) <br> Tainted LDAP Filter (Java) |
| CWE:909 | Missing Initialization of Resource | Empty jar File Archived (Java) <br> Empty zip File Archived (Java) |

| CWE:913 | Improper Control of Dynamically-Managed Code Resources | Insecure Class Loader (Java)<br>Deserializable Class (Java)<br>Deserializing Non-Serializable Class (Java)<br>Nonserializable Field Element (Java)<br>Nonserializable Field (Java)<br>Nonserializable Outer Class (Java)<br>Missing Serial Version Field (Java)<br>Unexpected Serial Version Field (Java) |
|---|---|---|
| CWE:915 | Improperly Controlled Modification of Dynamically-Determined Object Attributes | Reflection Bypasses Member Accessibility (Java)<br>Reflection Modifies Member Accessibility (Java) |
| CWE:916 | Use of Password Hash With Insufficient Computational Effort | Weak Cryptographic Value (Java)<br>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:1071 | Empty Code Block | Empty Branch Statement (Java) |
| CWE:1076 | Insufficient Adherence to Expected Conventions | compareTo in Non-Comparable Class (Java)<br>equals Parameter Should Be Object (Java) |
| CWE:1077 | Floating Point Comparison with Incorrect Operator | Floating Point Equality (Java) |
| CWE:1097 | Persistent Storable Data Element without Associated Comparison Control Element | Non-Object compareTo Parameter (Java) |
| CWE:1126 | Declaration of Variable with Unnecessarily Wide Scope | Unnecessary Field (Java) |
| CWE:1164 | Irrelevant Code | Unused Object (Java)<br>Field Never Read (Java)<br>Useless Class Cast (Java)<br>Redundant Implements Clause (Java)<br>Static Field Assigned Non-Static (Java)<br>Useless null Test (Java)<br>Useless null Test of Field (Java)<br>Useless null Test of Parameter (Java)<br>Redundant Call for String Argument (Java)<br>Unused Field (Java) |
| CWE:1173 | Improper Use of Validation Framework | Missing isValidFragment Override (Java) |
| CWE:1176 | Inefficient CPU Computation | Single-use Random Number Generator (Java) |
| CWE:1204 | Generation of Weak Initialization Vector (IV) | Weak Initialization Vector Field (Java)<br>Weak Initialization Vector Value (Java) |
| CWE:1339 | Insufficient Precision or Accuracy of a Real Number | Approximate e Constant (Java)<br>Approximate pi Constant (Java) |
| CWE:1390 | Weak Authentication | Anonymous LDAP Authentication (Java)<br>Authentication Disabled (Java) |

## CWE IDS THAT ARE BROADLY MAPPED TO ONE OR MORE CODESONAR JAVA WARNING CLASSES (CODESONAR V8.0)

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

| | | | | |
|---|---|---|---|---|
| CWE:19 | CWE:20 | CWE:22 | CWE:73 | CWE:74 |
| CWE:77 | CWE:78 | CWE:79 | CWE:81 | CWE:89 |
| CWE:90 | CWE:91 | CWE:93 | CWE:94 | CWE:95 |
| CWE:113 | CWE:114 | CWE:116 | CWE:117 | CWE:133 |
| CWE:134 | CWE:136 | CWE:137 | CWE:189 | CWE:190 |
| CWE:192 | CWE:197 | CWE:199 | CWE:200 | CWE:209 |
| CWE:221 | CWE:227 | CWE:252 | CWE:253 | CWE:254 |
| CWE:255 | CWE:259 | CWE:265 | CWE:284 | CWE:285 |
| CWE:287 | CWE:295 | CWE:310 | CWE:311 | CWE:319 |
| CWE:320 | CWE:321 | CWE:325 | CWE:326 | CWE:327 |
| CWE:328 | CWE:330 | CWE:335 | CWE:336 | CWE:338 |
| CWE:344 | CWE:345 | CWE:349 | CWE:361 | CWE:383 |
| CWE:388 | CWE:389 | CWE:390 | CWE:392 | CWE:395 |
| CWE:396 | CWE:397 | CWE:398 | CWE:399 | CWE:400 |
| CWE:404 | CWE:405 | CWE:411 | CWE:412 | CWE:413 |
| CWE:435 | CWE:436 | CWE:438 | CWE:440 | CWE:456 |
| CWE:465 | CWE:470 | CWE:471 | CWE:476 | CWE:477 |
| CWE:480 | CWE:481 | CWE:485 | CWE:486 | CWE:489 |
| CWE:491 | CWE:492 | CWE:501 | CWE:502 | CWE:522 |
| CWE:524 | CWE:538 | CWE:547 | CWE:550 | CWE:557 |
| CWE:561 | CWE:563 | CWE:567 | CWE:569 | CWE:570 |
| CWE:571 | CWE:572 | CWE:573 | CWE:580 | CWE:581 |
| CWE:582 | CWE:585 | CWE:586 | CWE:595 | CWE:597 |
| CWE:601 | CWE:607 | CWE:609 | CWE:610 | CWE:611 |
| CWE:613 | CWE:614 | CWE:624 | CWE:628 | CWE:629 |
| CWE:635 | CWE:642 | CWE:643 | CWE:657 | CWE:662 |
| CWE:664 | CWE:665 | CWE:666 | CWE:667 | CWE:668 |
| CWE:670 | CWE:671 | CWE:672 | CWE:674 | CWE:676 |
| CWE:681 | CWE:682 | CWE:684 | CWE:686 | CWE:690 |
| CWE:691 | CWE:693 | CWE:695 | CWE:697 | CWE:698 |
| CWE:699 | CWE:700 | CWE:703 | CWE:704 | CWE:705 |
| CWE:706 | CWE:707 | CWE:710 | CWE:711 | CWE:712 |
| CWE:713 | CWE:714 | CWE:715 | CWE:717 | CWE:718 |
| CWE:719 | CWE:720 | CWE:721 | CWE:722 | CWE:723 |
| CWE:724 | CWE:725 | CWE:726 | CWE:727 | CWE:728 |
| CWE:729 | CWE:730 | CWE:731 | CWE:732 | CWE:734 |
| CWE:735 | CWE:736 | CWE:737 | CWE:738 | CWE:739 |
| CWE:740 | CWE:741 | CWE:742 | CWE:743 | CWE:744 |
| CWE:745 | CWE:746 | CWE:747 | CWE:748 | CWE:749 |
| CWE:750 | CWE:751 | CWE:752 | CWE:753 | CWE:754 |
| CWE:755 | CWE:757 | CWE:768 | CWE:770 | CWE:771 |
| CWE:772 | CWE:789 | CWE:798 | CWE:800 | CWE:801 |
| CWE:802 | CWE:803 | CWE:808 | CWE:809 | CWE:810 |
| CWE:811 | CWE:812 | CWE:813 | CWE:815 | CWE:816 |
| CWE:817 | CWE:818 | CWE:819 | CWE:820 | CWE:821 |
| CWE:833 | CWE:834 | CWE:840 | CWE:844 | CWE:845 |
| CWE:846 | CWE:847 | CWE:848 | CWE:849 | CWE:850 |
| CWE:851 | CWE:852 | CWE:853 | CWE:854 | CWE:855 |
| CWE:857 | CWE:858 | CWE:859 | CWE:860 | CWE:861 |
| CWE:864 | CWE:865 | CWE:866 | CWE:867 | CWE:868 |
| CWE:871 | CWE:872 | CWE:873 | CWE:874 | CWE:875 |
| CWE:876 | CWE:877 | CWE:878 | CWE:879 | CWE:880 |
| CWE:882 | CWE:883 | CWE:884 | CWE:885 | CWE:886 |
| CWE:887 | CWE:888 | CWE:889 | CWE:890 | CWE:892 |
| CWE:893 | CWE:894 | CWE:895 | CWE:896 | CWE:897 |
| CWE:898 | CWE:899 | CWE:900 | CWE:902 | CWE:903 |
| CWE:905 | CWE:906 | CWE:907 | CWE:909 | CWE:913 |

| CWE:915 | CWE:916 | CWE:922 | CWE:928 | CWE:929 |
|---------|---------|---------|---------|---------|
| CWE:930 | CWE:931 | CWE:932 | CWE:933 | CWE:934 |
| CWE:935 | CWE:938 | CWE:943 | CWE:944 | CWE:945 |
| CWE:946 | CWE:947 | CWE:949 | CWE:950 | CWE:951 |
| CWE:957 | CWE:958 | CWE:959 | CWE:960 | CWE:961 |
| CWE:962 | CWE:963 | CWE:965 | CWE:966 | CWE:971 |
| CWE:975 | CWE:977 | CWE:978 | CWE:980 | CWE:981 |
| CWE:982 | CWE:983 | CWE:984 | CWE:985 | CWE:986 |
| CWE:987 | CWE:989 | CWE:990 | CWE:991 | CWE:992 |
| CWE:994 | CWE:997 | CWE:998 | CWE:1000 | CWE:1001 |
| CWE:1002 | CWE:1003 | CWE:1005 | CWE:1006 | CWE:1008 |
| CWE:1009 | CWE:1010 | CWE:1011 | CWE:1012 | CWE:1013 |
| CWE:1014 | CWE:1015 | CWE:1016 | CWE:1018 | CWE:1019 |
| CWE:1020 | CWE:1023 | CWE:1024 | CWE:1025 | CWE:1026 |
| CWE:1027 | CWE:1028 | CWE:1029 | CWE:1030 | CWE:1031 |
| CWE:1032 | CWE:1033 | CWE:1034 | CWE:1071 | CWE:1076 |
| CWE:1077 | CWE:1078 | CWE:1097 | CWE:1126 | CWE:1128 |
| CWE:1129 | CWE:1130 | CWE:1131 | CWE:1133 | CWE:1134 |
| CWE:1135 | CWE:1136 | CWE:1137 | CWE:1139 | CWE:1140 |
| CWE:1141 | CWE:1142 | CWE:1143 | CWE:1144 | CWE:1145 |
| CWE:1147 | CWE:1148 | CWE:1149 | CWE:1150 | CWE:1152 |
| CWE:1154 | CWE:1157 | CWE:1158 | CWE:1159 | CWE:1161 |
| CWE:1162 | CWE:1163 | CWE:1164 | CWE:1165 | CWE:1166 |
| CWE:1167 | CWE:1169 | CWE:1170 | CWE:1171 | CWE:1173 |
| CWE:1176 | CWE:1177 | CWE:1178 | CWE:1179 | CWE:1180 |
| CWE:1181 | CWE:1182 | CWE:1186 | CWE:1194 | CWE:1200 |
| CWE:1204 | CWE:1205 | CWE:1207 | CWE:1208 | CWE:1210 |
| CWE:1211 | CWE:1213 | CWE:1214 | CWE:1215 | CWE:1217 |
| CWE:1219 | CWE:1228 | CWE:1235 | CWE:1305 | CWE:1306 |
| CWE:1307 | CWE:1308 | CWE:1309 | CWE:1337 | CWE:1339 |
| CWE:1340 | CWE:1344 | CWE:1345 | CWE:1346 | CWE:1347 |
| CWE:1348 | CWE:1349 | CWE:1350 | CWE:1353 | CWE:1354 |
| CWE:1355 | CWE:1358 | CWE:1359 | CWE:1360 | CWE:1361 |
| CWE:1362 | CWE:1363 | CWE:1364 | CWE:1365 | CWE:1366 |
| CWE:1368 | CWE:1369 | CWE:1370 | CWE:1371 | CWE:1372 |
| CWE:1373 | CWE:1375 | CWE:1382 | CWE:1383 | CWE:1387 |
| CWE:1390 | CWE:1391 | CWE:1396 | CWE:1397 | CWE:1398 |
| CWE:1399 | CWE:1400 | CWE:1401 | CWE:1402 | CWE:1403 |
| CWE:1404 | CWE:1405 | CWE:1406 | CWE:1407 | CWE:1408 |
| CWE:1409 | CWE:1410 | CWE:1411 | CWE:1412 | CWE:1413 |
| CWE:1414 | CWE:1415 | CWE:1416 | CWE:1417 | CWE:1418 |
| CWE:1425 | | | | |