CWE-идентификаторы, которые включает в себя продукт, представлены в Таблице 1.

Таблица 1. Список CWE-идентификаторов продукта

|  |  |
| --- | --- |
| 14 | Удаление компилятором кода очистки буфера |
| 22 | Некорректное ограничение пути к директории. |
| 79 | Некорректная нейтрализация пользовательских данных, использующиеся для генерации web-страниц (XSS, межсайтовый скриптинг) |
| 89 | Некорректная нейтрализация специальных символов, используемых в SQL-запросах (SQL-инъекция) |
| 94 | Недостаточный контроль генерации кода (Инъекция кода) |
| 95 | Некорректная нейтрализация директив в динамически выполняемом кода (Eval-инъекция) |
| 103 | Неполное определение метода validate() |
| 113 | Некорректная нейтрализация CRLF последовательностей в HTTP-заголовках (Разделение HTTP-запросов) |
| 114 | Контроль процессов. |
| 117 | Некорректная фильтрация данных, попадающих в журналы. |
| 120 | Копирование буфера без проверки размера ввода (Классическое переполнение буфера) |
| 121 | Переполнение буфера на стеке |
| 125 | Чтение за пределами границ |
| 134 | Уязвимость форматной строки |
| 135 | Некорректное вычисление длины multi-byte строк |
| 170 | Некорректное завершение нулевым или эквивалентным символом |
| 194 | Непредсказуемое расширение знакозависимого типа. |
| 196 | Ошибки перевода беззнаковых типов в знакозависимые типы |
| 197 | Ошибки усечения чисел |
| 209 | Распространение информации через сообщения об ошибках |
| 213 | Умышленное раскрытие информации |
| 215 | Распространение информации через отладочные сообщения |
| 242 | Использование опасных функций |
| 245 | J2EE осуждаемое поведение, прямое управление соединениями |
| 252 | Непроверяемое возвращаемое значение |
| 253 | Некорректная проверка возвращаемого функцией значения |
| 259 | Использование жестко заданных паролей |
| 275 | Дефекты прав доступа |
| 312 | Хранение чувствительной информации в открытом виде |
| 327 | Использование нестойких криптографических алгоритмов |
| 337 | Предсказуемый инициализатор в ПГСЧ |
| 347 | Некорректная проверка криптографической подписи |
| 362 | Одновременное выполнение кода, использующего общий ресурс, при неправильной синхронизации ("Состояние гонки") |
| 369 | Деление на ноль |
| 375 | Возвращение изменяемого объекта недоверенному коду |
| 388 | Дефекты обработки ошибок |
| 390 | Пустой блок обработки условий и ошибок |
| 391 | Игнорирование ошибок |
| 395 | Перехват NullPointerException для обнаружения нулевого указателя |
| 397 | Объявление исключений общего вида |
| 398 | Признак плохого качества кода |
| 401 | Некорректное освобождение памяти перед удалением последней ссылки (Утечка памяти) |
| 404 | Некорректное освобождение ресурсов |
| 415 | Двойное освобождение области памяти |
| 428 | Небезопасный путь к файлу |
| 467 | Использование sizeof() с параметром в виде указателя |
| 468 | Некорректное операции с указателями |
| 476 | Разыменование нулевого указателя |
| 477 | Использование устаревших функций |
| 478 | Пропущенный default блок в switch выражении |
| 480 | Использование неверного оператора |
| 481 | Присваивание вместо сравнения |
| 482 | Сравнение вместо присваивания |
| 484 | Пропущенный break в switch выражениях |
| 486 | Сравнение классов по именам |
| 491 | Public метод cloneable() объявлен без модификатора final (Подмена объектов) |
| 497 | Выход системной информации в неконтролируемую область |
| 500 | Public static поле не объявлено как final |
| 506 | Встроенный вредоносный код |
| 511 | Логическая/временная бомба |
| 526 | Распространение информации через переменные среды |
| 545 | Использование динамической подгрузки классов |
| 557 | Дефекты многопоточности |
| 561 | Мёртвый код |
| 562 | Возврат адреса локальной переменной |
| 568 | Метод finalize() не вызывает super.finalize() |
| 569 | Проблемы, связанные с выражениями |
| 570 | Выражение всегда ложно |
| 571 | Выражение всегда истинно |
| 580 | Метод clone() не вызывает super.clone() |
| 581 | Нарушение объектной модели: определён только equals() или только hashcode() |
| 582 | Массив объявлен public, final и static |
| 583 | Метод finalize() объявлен как public |
| 584 | Выражение возврата внутри finally блока |
| 585 | Пустой блок синхронизации |
| 586 | Принудительный вызов finalize() |
| 587 | Присвоение фиксированного адреса указателю |
| 590 | Освобождение памяти не из кучи |
| 606 | Недоверенные данные в условии цикла |
| 609 | Двойная блокировка ресурса |
| 617 | Достижимое assert() выражение |
| 628 | Вызов функции с некорректными аргументами |
| 648 | Некорректное использование API работы с привилегиями |
| 662 | Неправильная синхронизация |
| 674 | Неконтролируемая рекурсия |
| 682 | Некорректные вычисления |
| 683 | Передача аргументов функции в неправильном порядке |
| 691 | Недостаточный контроль над потоком управления. |
| 697 | Неверное сравнение |
| 730 | OWASP топ-10 2004 категория A9 - Отказ в обслуживании |
| 759 | Использование хэширования без соли |
| 770 | Неконтролируемое выделение ресурсов |
| 780 | Использование алгоритма RSA без OAEP |
| 798 | Использование жестко заданных учетных данных |
| 806 | Использование размера исходного буфера для записи в буфер назначения |
| 835 | Цикл с недосягаемым условием выхода (Бесконечный цикл) |
| 858 | CERT Java Secure Coding Section 13 - Сериализация (SER) |
| 961 | SFP Вторичный кластер: Неверное поведение исключений |

Table 1 presents CWE identifiers, included in the product.

Table 1. A list of CWE identifiers in the product

|  |  |
| --- | --- |
| 14 | Compiler Removal of Code to Clear Buffers |
| 22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| 79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| 89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
| 94 | Improper Control of Generation of Code ('Code Injection') |
| 95 | Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') |
| 103 | Struts: Incomplete validate() Method Definition |
| 113 | Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') |
| 114 | Process Control |
| 117 | Improper Output Neutralization for Logs |
| 120 | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') |
| 121 | Stack-based Buffer Overflow |
| 125 | Out-of-bounds Read |
| 134 | Uncontrolled Format String |
| 135 | Incorrect Calculation of Multi-Byte String Length |
| 170 | Improper Null Termination |
| 194 | Unexpected Sign Extension |
| 196 | Unsigned to Signed Conversion Error |
| 197 | Numeric Truncation Error |
| 209 | Information Exposure Through an Error Message |
| 213 | Intentional Information Exposure |
| 215 | Information Exposure Through Debug Information |
| 242 | Use of Inherently Dangerous Function |
| 245 | J2EE Bad Practices: Direct Management of Connections |
| 252 | Unchecked Return Value |
| 253 | Incorrect Check of Function Return Value |
| 259 | Use of Hard-coded Password |
| 275 | Permission Issues |
| 312 | Cleartext Storage of Sensitive Information |
| 327 | Use of a Broken or Risky Cryptographic Algorithm |
| 337 | Predictable Seed in PRNG |
| 347 | Improper Verification of Cryptographic Signature |
| 362 | Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |
| 369 | Divide By Zero |
| 375 | Returning a Mutable Object to an Untrusted Caller |
| 388 | Error Handling |
| 390 | Detection of Error Condition Without Action |
| 391 | Unchecked Error Condition |
| 395 | Use of NullPointerException Catch to Detect NULL Pointer Dereference |
| 397 | Declaration of Throws for Generic Exception |
| 398 | Indicator of Poor Code Quality |
| 401 | Improper Release of Memory Before Removing Last Reference ('Memory Leak') |
| 404 | Improper Resource Shutdown or Release |
| 415 | Double Free |
| 428 | Unquoted Search Path or Element |
| 467 | Use of sizeof() on a Pointer Type |
| 468 | Incorrect Pointer Scaling |
| 476 | NULL Pointer Dereference |
| 477 | Use of Obsolete Functions |
| 478 | Missing Default Case in Switch Statement |
| 480 | Use of Incorrect Operator |
| 481 | Assigning instead of Comparing |
| 482 | Comparing instead of Assigning |
| 484 | Omitted Break Statement in Switch |
| 486 | Comparison of Classes by Name |
| 491 | Public cloneable() Method Without Final ('Object Hijack') |
| 497 | Exposure of System Data to an Unauthorized Control Sphere |
| 500 | Public Static Field Not Marked Final |
| 506 | Embedded Malicious Code |
| 511 | Logic/Time Bomb |
| 526 | Information Exposure Through Environmental Variables |
| 545 | Use of Dynamic Class Loading |
| 557 | Concurrency Issues |
| 561 | Dead Code |
| 562 | Return of Stack Variable Address |
| 568 | finalize() Method Without super.finalize() |
| 569 | Expression Issues |
| 570 | Expression is Always False |
| 571 | Expression is Always True |
| 580 | clone() method does not call super.clone() |
| 581 | Object Model Violation: Just One of Equals and Hashcode Defined |
| 582 | Array Declared Public, Final, and Static |
| 583 | finalize() Method Declared Public |
| 584 | Return Inside Finally Block |
| 585 | Empty Synchronized Block |
| 586 | Explicit Call to Finalize() |
| 587 | Assignment of a Fixed Address to a Pointer |
| 590 | Free of Memory not on the Heap |
| 606 | Unchecked Input for Loop Condition |
| 609 | Double-Checked Locking |
| 617 | Reachable Assertion |
| 628 | Function Call with Incorrectly Specified Arguments |
| 648 | Incorrect Use of Privileged APIs |
| 662 | Improper Synchronization |
| 674 | Uncontrolled Recursion |
| 682 | Incorrect Calculation |
| 683 | Function Call With Incorrect Order of Arguments |
| 691 | Insufficient Control Flow Management |
| 697 | Insufficient Comparison |
| 730 | OWASP Top Ten 2004 Category A9 - Denial of Service |
| 759 | Use of a One-Way Hash without a Salt |
| 770 | Allocation of Resources Without Limits or Throttling |
| 780 | Use of RSA Algorithm without OAEP |
| 798 | Use of Hard-coded Credentials |
| 806 | Buffer Access Using Size of Source Buffer |
| 835 | Loop with Unreachable Exit Condition ('Infinite Loop') |
| 858 | CERT Java Secure Coding Section 13 - Serialization (SER) |
| 961 | SFP Secondary Cluster: Incorrect Exception Behavior |