Общество с ограниченной ответственностью
"АН-СЕКЬЮРИТИ КИБЕР-БЕЗОПАСНОСТЬ"
195027, Санкт-Петербург, ул. Конторская, д.11, литера А, офис 421
+7 (812) 318 4000, доб. 2222
an-cyber.ru

Fragile.NET

Анализатор уязвимостей

руководство пользователя

Для запуска программного продукта «Fragile.NET» требуется перейти в каталог, в которую она была загружена, и запустить файл Analyzer.exe.

Графический пользовательский интерфейс представляет из себя единственное окно с возможностью указания файла для анализа и область вывода отчёта.

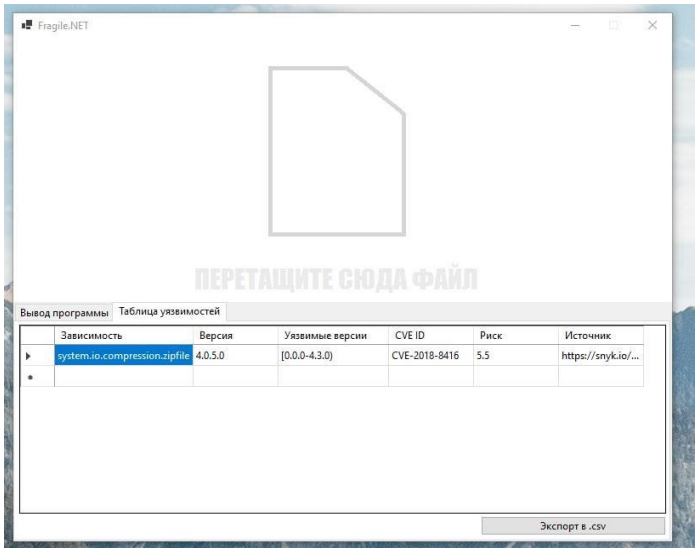

Рис. 1. Общий вид пользовательского интерфейса.

После указания файла и успешного его анализа программой, в области вывода отчёта отображается подробная информация о результате анализа. В случае ошибки анализа файла, выводится подробная информация об ошибке.

Каждая строка таблицы уязвимостей соответствует одной найденной уязвимой зависимости.
Столбцы таблицы уязвимостей:

- Зависимость - название зависимости. Обычно здесь отображается пространство имён (namespace) подключенной библиотеки, позволяя однозначно её идентифицировать.
- Версия - используемая анализируемой сборкой версия зависимости.
- Уязвимые версии - диапазон всех известных версий этой библиотеки, имеющих ту же уязвимость, которую содержит используемая сборкой версия.
- CVE ID - уникальный идентификатор уязвимости в базе Common Vulnerabilities and Exposures (https://cve.mitre.org/).
- Риск - степень вредоносного потенциала уязвимости по шкале от 1 (низкая) до 10 (высокая) по оценке специалистов сайта https://snyk.io. ● Источник - ссылка на страницу, откуда были взяты данные об этой уязвимости.

Для передачи на вход анализируемого файла в консольном режиме, требуется передать путь к этому файлу в качестве первого аргумента программы. Предпочтительнее использовать графический пользовательский интерфейс.

Для передачи на вход анализируемого файла через графический пользовательский интерфейс, требуется нажать на кнопку “Выбрать файл” и указать файл, который требуется проанализировать

В результате работы ПП генерирует отчет, содержащий:

- название зависимости (сборки);
- версию сборки;
- уязвимые версии этой сборки;
- CVE ID;
- уровень риска;
- источник сведений об уязвимости.

Данные можно просмотреть в окне программы, а также выгрузить в формате таблицы (файл CSV).

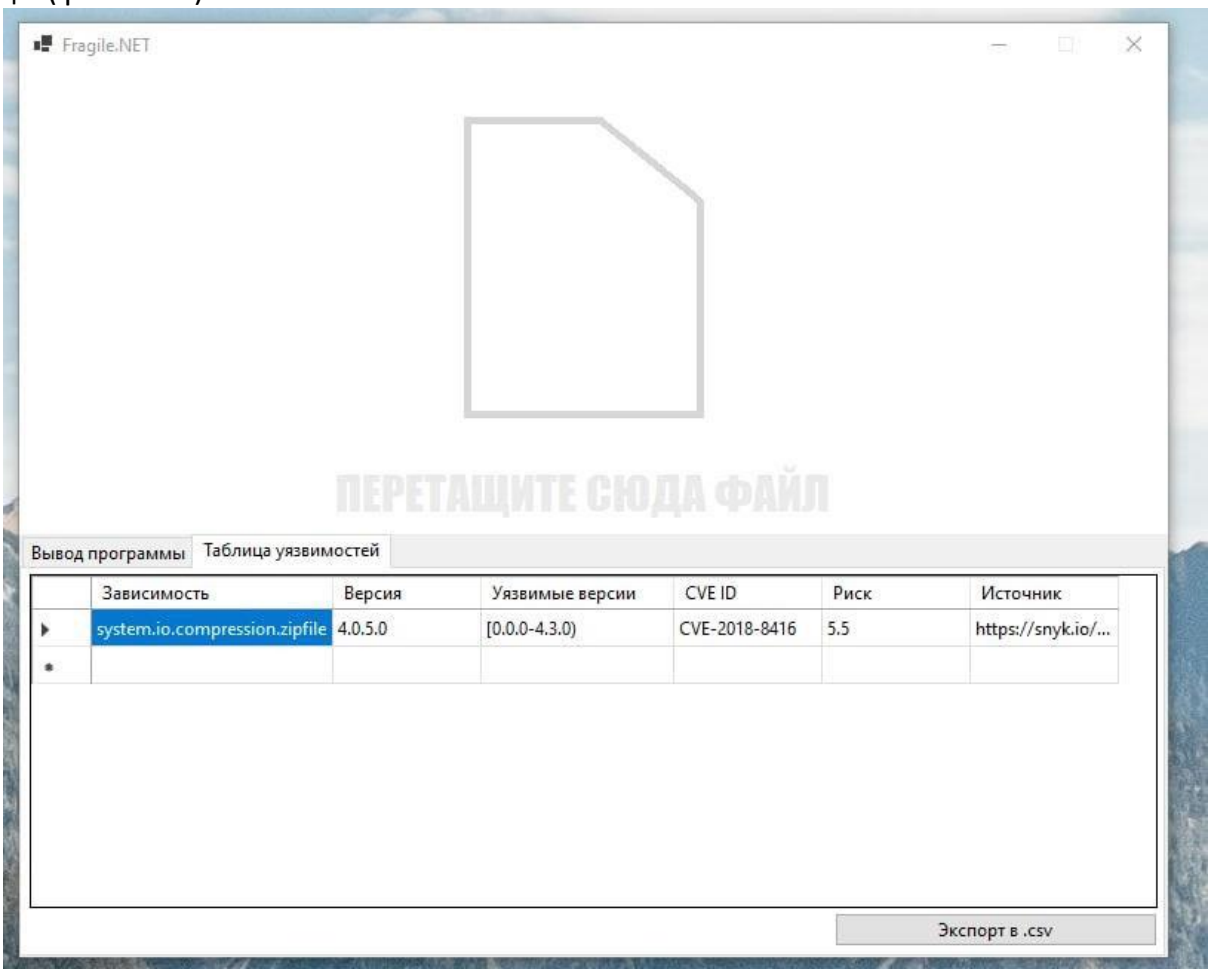

Рис. 3. Результат выполнения анализа - таблица с отчетом, которую возможно экспортировать в CSV-файл.