Отчет о статическом анализе кода

Общая информация о тестировании:
Отчет содержит результаты проведенных работ по статическому анализу кода (далее – Система) компании АО «XXXX», выполненных в соответствии с договором от _____ г. № XXXX, заключенным между Исполнителем и АО «XXX». В отчете содержится описание выявленных недостатков и связанных с ними уровней критичности.
Объект тестирования: ссылка на код
Тестирование провел: Вишняк Е. И.
Методика проведения тестирования:
SAST-сканирование с использованием Sonarqube
Дата: 12.07.2024

Обнаруженные уязвимости:

Название	Описание	Вероятность эксплойта	Ссылка
CWE-327: Use of a Broken or Risky Cryptographic Algorithm	Криптографические алгоритмы - это методы, с помощью которых данные шифруются для предотвращения наблюдения или влияния со стороны неавторизованных лиц. Слабая криптография может быть использована для раскрытия конфиденциальной информации, изменения данных неожиданным образом, имитации личности других пользователей или устройств, или других последствий. Очень сложно создать безопасный алгоритм, и даже алгоритмы высокого уровня, разработанные опытными экспертами по криптографии, были взломаны. Известны методы взлома или ослабления различных видов криптографии. Соответственно,	High	https://cwe.mitre.org/data/definitions/327.html

	существует небольшое количество хорошо понятных и тщательно изученных алгоритмов, которые должны использоваться в большинстве продуктов. Использование нестандартного или известного небезопасного алгоритма опасно, потому что решительный противник может взломать алгоритм и скомпрометировать защищенные данные. Поскольку состояние криптографии быстро развивается, часто бывает так, что алгоритм считается "небезопасным", даже если когда-то считалось, что он сильный. Это может произойти, когда выявляются новые атаки или если вычислительная мощность увеличивается настолько, что криптографический алгоритм больше не обеспечивает уровень защиты, который изначально считался высоким. По ряду причин, этой уязвимостью еще сложнее управлять при аппаратной реализации криптографических алгоритмов по сравнению с программной реализацией. Во-первых, если обнаружена ошибка в аппаратно реализованной криптографии, ее нельзя исправить в большинстве случаев без отзыва продукта, поскольку аппаратное обеспечение не так легко заменить, как программное обеспечение. Во-вторых, поскольку ожидается, что продукт будет работать в течение нескольких лет, вычислительная мощность противника будет только увеличиваться со временем, что говорит о потенциальной угрозе.		

CWE-326: Inadequate Encryption Strength	Слабый шифровальный алгоритм может быть подвержен атакам методом грубой силы, которые имеют разумные шансы на успех с использованием текущих методов атаки и ресурсов.		https://cwe.mitre.org/data/definitions/326.html
CWE-297: Improper Validation of Certificate with Host Mismatch	Даже если сертификат правильно сформирован, подписан и соответствует цепочке доверия, он может быть действительным сертификатом для другого сайта, чем тот, с которым взаимодействует продукт. Если хост-специфичные данные сертификата не проверяются должным образом - например, Общее имя (CN) в Субъекте или Расширение Альтернативного имени Субъекта (SAN) сертификата X.509 - возможно, что перенаправление или атака спуфинга позволит злонамеренному хосту с действительным сертификатом предоставить данные, выдавая себя за доверенный хост. Чтобы гарантировать целостность данных, сертификат должен быть действительным и относиться к сайту, к которому осуществляется доступ. Даже если продукт пытается проверить имя хоста, все равно возможны ошибки при проверке. Например, злоумышленники могут создать сертификат с именем, начинающимся с доверенного имени, за которым следует байт NUL, что может привести к тому, что некоторые строковые сравнения будут рассматривать только ту часть, которая содержит доверенное имя. Эта уязвимость может возникнуть даже тогда, когда продукт использует привязку	High	https://cwe.mitre.org/data/definitions/297.html

	сертификатов, если продукт не проверяет имя хоста в момент привязки сертификата.		
CWE-295: Improper Certificate Validation	Когда сертификат недействителен или вредоносный, он может позволить злоумышленнику имитировать доверенное лицо, внедряясь в путь связи между хостом и клиентом. Продукт может подключиться к злонамеренному хосту, полагая, что это доверенный хост, или продукт может быть введен в заблуждение, приняв поддельные данные, которые кажутся исходящими от доверенного хоста.		https://cwe.mitre.org/data/definitions/295.html
CWE-780: Use of RSA Algorithm without OAEP	Схема дополнения часто используется с криптографическими алгоритмами для того, чтобы сделать открытый текст менее предсказуемым и усложнить задачу атакующему. Схема OAEP часто используется с RSA для нейтрализации воздействия предсказуемости открытого текста.	Medium	https://cwe.mitre.org/data/definitions/780.html