Развитие Методики выявления уязвимостей и недекларированных возможностей в контексте типовых ошибок и недочетов при подготовке и проведении испытаний

Дмитрий Пономарев

технический директор **ООО НТЦ «Фобос-НТ»**
сотрудник **ИСП РАН**

@DmitryJustDmitry

Преамбула. Методический сбор ФСТЭК России с ИЛ и ОС (30 ноября 2022 г.)

- Некорректное определение поверхности атаки:
  - в поверхность атаки не включены интерфейсы, не реализующие функции безопасности
  - в поверхность атаки не включены модули взаимодействия с файловыми системами носителей информации
  - на сайте разработчика указан функционал СЗИ, не исследуемый при сертификационных испытаниях, при этом потенциально входящий в поверхность атаки

- Не описан режим работы и настройки фаззера
- Не проанализированы сбои в работе фаззера, не описаны исправления исходных кодов по результатам анализа сбоев
- В электронных приложениях не приведены логи проверок инструментальными средствами, отчеты о покрытии, сэмплы, словари
- В протоколе испытаний недостаточно подробно описаны испытания - не приведены конкретные скриншоты из логов в электронных приложениях и реальных окон работы программ анализа

Среда функционирования		
Операционные системы	**Системы управления базами данных**	**Интерпретаторы**
Хотя бы одна сертифицированная ОС в составе среды функционирования	Должны быть сертифицированы или входить в состав объекта оценки	

- Не проанализированы модули, реализующие среду выполнения интерпретируемого кода или кода, компилируемого в промежуточное представление
- Не представлена информация о исправлении разработчиком всех ошибок критического/высокого уровня опасности, оцененных ИЛ как истинные
- Не представлен план по исправлению ошибок

- Не приведено краткое описание того, каким инструментом и с какими настройками выполняется анализ уязвимостей
- Не приведено подтверждение хода исследования на основе логов/скриншотов
- По всем выявленным значимым проблемам не представлены обоснования неэксплуатируемости, либо подтверждения того, что уязвимость устранена (логи, скриншоты)

Преамбула. Основные системные проблемы заявителей с позиции ИЛ

- некорректное определение либо сведение к минимуму поверхности атаки, в том числе в парадигме «организационных мер»
    - особенно в случае СЗИ в контейнерном исполнении
- нарушение принципа «за всю кодовую базу кто-то должен отвечать», бесконтрольное переиспользование компонентов из репозиториев сертифицированных ОС
    - слабый контроль за известными уязвимостями, особенно для контейнеров
- отсутствие единых стандартов представления результатов анализа, затрудняющее работу всех этапов контроля
- выполнение практик «в общем», без мотивации найти и исправить найденные проблемы

Вместо оглавления

Блок №1. Структурные изменения документа

Блок №2. Ответственность за сторонние (заимствуемые и привлекаемые) компоненты

Блок №3. Поверхность атаки

Блок №4. Некоторые технологические аспекты

Блок №5. Распределение обязанностей и Центры компетенций

Три тезиса к основной части доклада

Приведённые далее цитаты не являются выдержками из финализированного нормативного документа, но демонстрируют тенденции проекта совершенствования Методики ВУ и НДВ.

Целевой функцией является создание нормативного документа, который будет понятен непосредственно инженеру-исполнителю без привлечения «толмача» из группы сертификации.

Возможность перечислить все частные случаи в едином документе, и одновременно обеспечить актуальность и удобство его использования, полагается практически нереализуемой. В тех случаях, когда вам не хватает «букв закона», ориентируйтесь на его дух – стремление разрабатывать безопасный и **качественный** код!

Блок №1. Структурные изменения документа

Блок №1. Недостаточная структурированность документа

Проблемы

- в актуальной версии Методики ВУ и НДВ в ряде случаев несколько рекомендаций смешаны в один абзац, либо рекомендация «размыта» на несколько абзацев. Отсутствие четких атомарных требований и рекомендаций затрудняет планирование и контроль за испытаниями, построение стандартизованной отчетности с привязкой разделов отчетных материалов к разделам методики

- в ряде случаев в одном абзаце смешаны требования различных этапов (планирование, испытание, контроль результатов)

Подходы к решению

- явно выделить минимально-необходимые требования к испытаниям

- каждое требование получает уникальный идентификатор (номер)

- для каждой практики введены подготовительный, результирующий подразделы

Блок №1. Недостаточная структурированность документа

Прототип решения

4.1.1.3.40. Требуется выполнить анализ исходного текста ОО в части комментариев разработчика к исходному тексту, направленный на выявление потенциально опасных функциональных возможностей и НДВ.

4.1.1.3.50. Требуется выполнить анализ исходного текста ОО, направленный на выявление в исходных текстах открыто присутствующей чувствительной информации и «секретов» (пароли, приватные ключи и т. п.).

4.1.1.3.60. Требуется выполнить автоматизированный анализ настроек ОО и отдельных модулей, составляющих ОО, направленный на выявление уязвимостей конфигурации ОО. Для контроля настроек ОО применяются инструментальные средства анализа конфигураций, при наличии таковых средств.

4.1.1. Анализ архитектуры ОО статическими методами (КАО.1)

4.1.1.1. Задачи исследования

Задачей исследования является выявление в ОО:

- потенциально опасных функциональных возможностей;
- недекларированных возможностей;
- архитектурных уязвимостей;
- уязвимостей конфигурации;

и иных, в том числе публично известных, уязвимостей методами и инструментами, не требующими выполнения кода ОО.

4.1.1.2. Исходные данные исследования

Исходными данными при проведении исследования являются:

- исходные данные в соответствии с требованиями пункта 2.4 Методики;
- результаты анализа разработчиком безопасности архитектуры и скрытых каналов ОО;
- сведения, полученные по результатам анализа документации и иных исходных данных (ПОД.1);
- исходные тексты ОО;
- система автоматизации сборки ОО.

Блок №1. Недостаточная структурированность документа

Проблемы

- в актуальной версии Методики ВУ и НДВ в ряде случаев отсутствуют явные требования к минимальной результирующей отчетности

Подходы к решению

- явно ввести требования к минимальной результирующей отчетности

Блок №1. Недостаточная структурированность документа

Прототип решения

4.3.1.5.20. Требуется зафиксировать в протоколах испытаний параметры сборки фаззинг-цели, принцип формирования коллекции, правил, словарей, достигнутое структурное покрытие по строкам исходного текста или по базовым блокам исполняемого кода для каждого фаззинг-цели, логи фаззинг-тестирования.

Блок №1. Недостаточная структурированность документа

Проблемы

- в актуальной версии Методики ВУ и НДВ, в силу исторических причин правило разнесения активностей вида «архитектурный анализ» по блокам КАО.1 и КАО.2 в ряде случаев неявно

Подходы к решению

- ввести явное правило классификации активностей вида «архитектурный анализ» по принадлежности к блокам КАО.1 и КАО.2

Прототип решения

4.1. Анализ архитектуры объекта оценки (КАО)

Анализ архитектуры ОО включает:

а) анализ архитектуры ОО статическими методами (КАО.1);

б) анализ архитектуры ОО динамическими методами (КАО.2).

Блок №1. Недостаточная структурированность документа

Проблемы

- в актуальной версии Методики ВУ и НДВ присутствует текстовая избыточность

- в актуальной версии Методики ВУ и НДВ раздел 2 (общий предварительный) раздел в меньшей степени являлся конкретным руководством к действию, фактически являясь «мертвым» текстом «за всё хорошее»

Подходы к решению

- дополнить раздел 2 более конкретными процессными рекомендациями

- вынести в раздел 2 некоторые общие практики, далее ссылаться на них по тексту Методики ВУ и НДВ

Блок №1. Недостаточная структурированность документа

Прототип решения

2.13. Сведения обо всех выявленных уязвимостях заимствуемых и привлекаемых компонент, а также уязвимостях, актуальных для ранее сертифицированных версий ОО и собственных компонент ОО, направляются испытательной лабораторией во ФСТЭК России в формате и порядке взаимодействия с БДУ ФСТЭК России.

2.14. Разработанные меры по устранению уязвимостей, ПОФВ и НДВ ОО подлежат исследованию на предмет корректности, а также с целью контроля отсутствия новых уязвимостей, ПОФВ и НДВ ОО, которые могли быть внесены в ОО в результате устранения. Повторное исследование в полном объеме предписанных практик и методик (в том числе функционального тестирования) требуется выполнять только в отношении исходного текста и исполняемого (интерпретируемо) кода ОО, прямо или косвенно затронутых внесенными изменениями.

2.15. Отказ разработчика от устранения актуальных уязвимостей, ПОФВ и НДВ ОО является основанием для выдачи отрицательного заключения о результатах сертификационных испытаний.

2.16. Не требуется фиксировать значения контрольных сумм дистрибутива, исполняемых файлов и файлов исходных текстов (в соответствии с уровнем контроля) ОО в документации ОО и акте отбора образцов ОО до момента успешного завершения испытаний ОО. Дистрибутив ОО, подвергаемый испытаниям, считается промежуточным (не эталонным) до момента успешного

завершения испытаний ОО. Предоставление эталонного дистрибутива и

Блок №2. Ответственность за сторонние (заимствуемые и привлекаемые) компоненты

Блок №2. Ответственность за сторонние компоненты

Проблемы

- использование в составе СЗИ связанных с реализацией функций безопасности бинарных файлов, не собираемых из исходных кодов, даже при испытаниях по 6 уровню контроля

- **в том числе в составе образов контейнеров, как правило выкачанных из Docker Registry!**

Подходы к решению

- ввести требования по обязательности предоставления всех исходных кодов СЗИ (за исключением частных случаев) и выполнению сборки СЗИ из представленных исходных кодов

Блок №2. Ответственность за сторонние компоненты

Прототип решения

2.4. Для выявления уязвимостей, ПОФВ и НДВ ОО разработчиком ОО, в соответствии с уровнем контроля, по которому проводятся испытания, представляются в испытательную лабораторию следующие исходные данные:

а) документация на ОО (а именно: технические условия или техническое задание; формуляр; программная (конструкторская) документация, содержащая сведения об архитектуре программ, процедурах передачи программного обеспечения пользователю, функциональные спецификации; эксплуатационная документация (руководство пользователя, руководство администратора), а также иные документы на ОО, разработка которых предусмотрена в соответствии с Требованиями к уровням доверия);

б) исходный текст объекта оценки, за исключением 6 уровня контроля;

Блок №2. Ответственность за сторонние компоненты

Проблемы

- отсутствие стандартного механизма учёта сторонних (заимствуемых и привлекаемых) компонентов, позволяющего Регулятору выполнять автоматическую связку с БДУ ФСТЭК в части выявления известных уязвимостей с сертифицированных СЗИ, а также анализировать использование сторонних компонентов

Подходы к решению

- введение концепции Реестра компонентных связей (aka Bill of Materials)

Блок №2. Ответственность за сторонние компоненты

Прототип решения

ж) сведения о сторонних программных компонентах, составляющих ОО (далее - заимствуемые программные компоненты) и среду его функционирования (далее – привлекаемые программные компоненты), в том числе динамически компонуемых библиотеках; средах функционирования интерпретируемых языков или языков, компилируемых в промежуточное представление; системах управления базами данных и иных; в объеме и форме представления, приведенных в Приложении 8;

Нотация представления заимствуемых и привлекаемых компонент в машиночитаемом формате

А. Цели создания машиночитаемой нотации профиля СЗИ

- стимулирование внедрения автоматических трекеров известных уязвимостей в CI-процессы разработчика;

- автоматизированное оперативное выявление СЗИ, содержащих предположительно уязвимые пакеты (обогащение на фиде БДУ), и последующий контроль устранения их разработчиком (включает в себя взаимодействие с потребителями, и оповещение БДУ о выявленных уязвимостях в СЗИ), а также своевременного и регулярного прохождения испытаний в связи с внесением изменений;

- автоматизированная поддержка при оценке полноты испытаний по принципу сравнения того, как X разработчиков проводят работы в отношении пакета Y, определяют поверхность атаки в отношении сходных СЗИ, а также подходят к устранению уязвимостей;

Блок №2. Ответственность за сторонние компоненты

Проблемы

- нарушение принципа «за всю кодовую базу кто-то должен отвечать», бесконтрольное переиспользование компонентов из репозиториев сертифицированных ОС

Подходы к решению

- введение методологии формального прослеживания истории компонентов относительно репозиториев сертифицированных ОС

Блок №2. Ответственность за сторонние компоненты

Прототип решения

з) сведения о прохождении составляющими ОО сторонними программными компонентами испытаний, в случае переиспользования данных компонент из состава дистрибутива, ранее сертифицированного по соответствующему уровню контроля. Сведения должны быть представлены в объеме, допускающем экспертную верификацию, например:

- документ и пункт в эксплуатационной документации сертифицированного дистрибутива (например: комплектность поставки), содержащий упоминание компонента в числе подлежащих переиспользованию компонент;
- номер и дата протокола сертификационных испытаний дистрибутива, в ходе которых подлежащий переиспользованию компонент подвергался испытаниям.

Блок №2. Ответственность за сторонние компоненты

Проблемы

- как правило при выходе на испытания оказывается, что многие сторонние компоненты, составляющие кодовую базу СЗИ, содержат известные уязвимости. Основные причины:
  - разработчик вообще не знал, что так нужно было: «лишь бы сдать работу»
  - у разработчика не внедрена автоматизированная/автоматическая система отслеживания известных уязвимостей

- **в том числе в составе образов контейнеров!**

Подходы к решению

- введение методологии формального прослеживания истории компонентов относительно репозиториев сертифицированных ОС

Блок №2. Ответственность за сторонние компоненты

Прототип решения

4.1.1.3.20. Требуется выполнить поиск известных уязвимостей сторонних (заимствуемых) компонентов ОО и сред его функционирования, в том числе компонентов, формирующих контейнеры для СЗИ в контейнерном исполнении, в публично доступных базах уязвимостей с учетом сведений об исходных репозиториях модулей, названиям, версиям модулей, включая платформенно-зависимые идентификаторы (Common Platform Enumeration).

4.1.1.3.30. Требуется убедиться во внедрение разработчиком систем (в частности: CodeClones, OWASP Dependency Track, OWASP Dependency Check, CodeScoring и т. п.) автоматизированного поиска известных уязвимостей в сторонних (заимствуемых) компонентах, в случае если число таковых компонентов превышает 20 единиц.

Блок №3. Поверхность атаки

Блок №3. Поверхность атаки

Проблемы

- разработчики всячески стремятся уйти от анализа низкоуровневого и специализированного кода, мотивируя это тем, что «обещана отдельная Методика ФСТЭК России и пока её нет, то на нет и суда нет…»

Подходы к решению

- явно прописать, что код – даже если он низкоуровневый – следует анализировать с опорой на имеющиеся инструменты и методики, в случае как минимум частичной их применимости

Прототип решения

1.2. Методика определяет требования к составу и содержанию исследований по выявлению уязвимостей и недекларированных возможностей в программных компонентах общесистемного, прикладного программного обеспечения и средств защиты информации (далее – объект оценки, ОО), в том числе доступных в исходных текстах компонентах драйверов, базовых систем ввода-вывода, средств доверенной загрузки, средств контроля носителей, гипервизоров, а также применяемым при этом методам исследований и инструментальным средствам анализа и контроля.

Блок №3. Поверхность атаки

Проблемы

- разработчики в ходе сертификационных испытаний всячески преуменьшают поверхность атаки

- в том числе «забывают» про сервисы, не включенные по умолчанию, но входящие в состав дистрибутива

- в том числе забывают, что практически все пользователи – даже низкопривилегированные администраторы – это потенциальные нарушители

Подходы к решению

- ещё более явно описать подход к определению поверхности атаки

Блок №3. Поверхность атаки

Прототип решения

3.1.3.20. Требуется выполнить анализ поверхности атаки ОО, предусматривающий определение внешних интерфейсов ОО, непосредственно доступных потенциальным нарушителям, и модулей ОО, реализующих обработку данных, поступающие по данным интерфейсам. К внешним интерфейсам ОО, непосредственно доступным для атаки потенциальным нарушителям, относятся все интерфейсы всех потенциально возможных совокупностей режимов безопасного функционирования ОО, для которых одновременно выполняются

Интерфейсы, доступные пользователям, обладающим административной ролью, допускающей настройку набора привилегий, относятся к интерфейсам ОО, доступным для атаки потенциальными нарушителем из числа низкопривилегированных администраторов (например: к сетевому веб-интерфейсу администрирования ОО имеют доступ все пользователи, обладающие ролью «Администратор». При этом возможность доступа пользователя к

Блок №3. Поверхность атаки

Проблемы

- разработчики и эксперты стремятся «изобразить» исследования (в первую очередь это относится к фаззингу, но не только) вместо того, чтобы действительно применять Методику для поиска уязвимостей. Одним из явных проявлений является попытка выполнять динамическое тестирование сложных алгоритмов без декомпозиции реализующего алгоритм программного кода на составные части (парсеры, анализаторы) и выполнения их прецизионного анализа

Подходы к решению

- явно обозначить необходимость прецизионного анализа некоторых участков кода и дать рекомендации по их выявлению в общем массиве кода СЗИ

Прототип решения

3. Требуется выделить в составе модулей поверхности атаки участки кода, наиболее плотно взаимодействующие с данными, поступающими от потенциального нарушителя (парсеры, анализаторы; в том числе в составе кода веб-приложений), и имеющие высокую цикломатическую сложность, для последующего формирования на их основе синтетических целей для фаззинг-тестирования. Состав выделенных целей подлежит уточнению непосредственно в ходе проведения испытаний с фиксацией выделенных целей в протоколах испытаний, без требования внесения изменений в методику испытаний.

Блок №3. Поверхность атаки

Проблемы

- разработчики и эксперты стремятся свести к минимуму поверхность атаки в случае определения её только «экспертным» методом

Подходы к решению

- нужно больше автоматических средств и методик определения поверхности атаки

Прототип решения

2. Требуется верифицировать определенную в ходе выполнения ПОД.1 поверхность атаки ОО с использованием средств трассировки приложений пользовательского режима выполнения или средств интроспекции виртуальных машин, в случае если определение поверхности атаки ОО выполнялось экспертным методом без привлечения инструментальных средств.

Блок №3. Поверхность атаки

Проблемы

- отсутствие единого стандарта отображения поверхности атаки между командами одного разработчика и между участниками системы сертификации критически усложняет оценку регулятором результатов испытаний в плане полноты анализа поверхности атаки

Подходы к решению

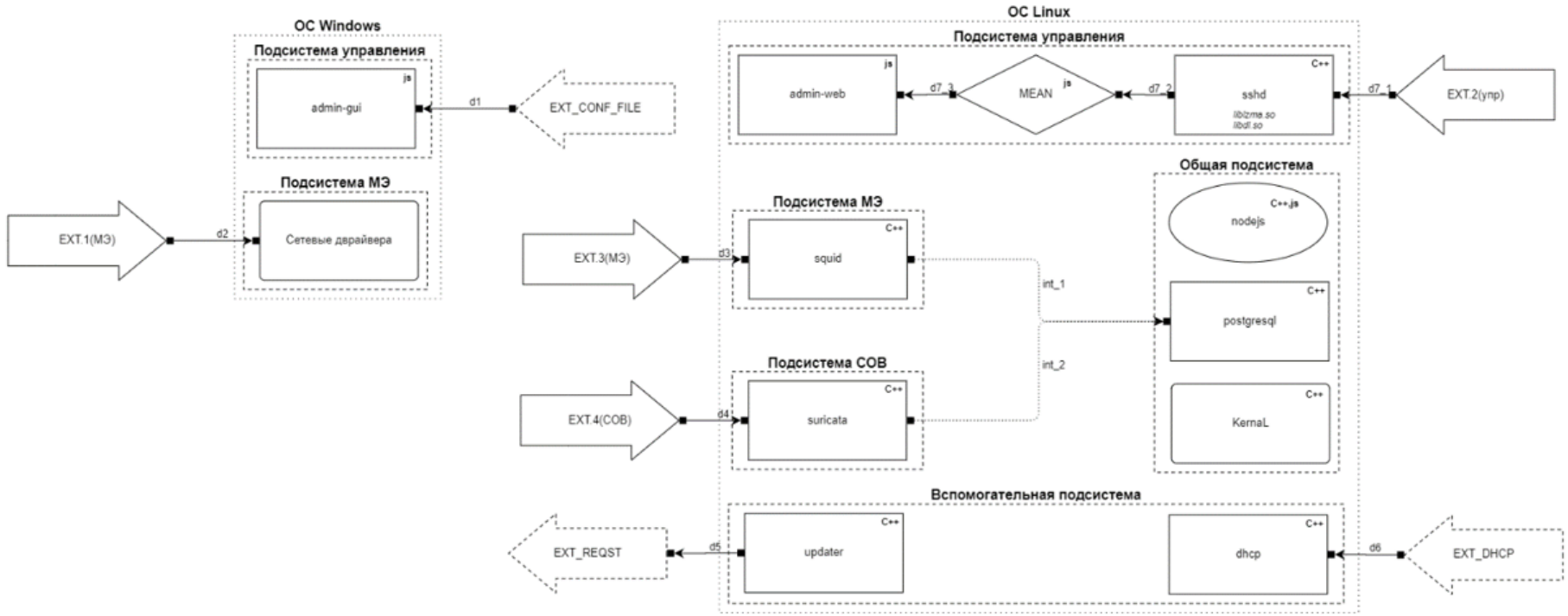
- требуется единая машиночитаемая нотация отображения архитектуры разнотиповых и разномасштабных объектов оценки, в том числе в рамках выполнения Требований Доверия разработчиком

Блок №3. Поверхность атаки

Прототип решения

3.1.5.20. Требуется зафиксировать в методике (протоколе) испытаний сведения о поверхности атаки в нотации, приведенной в Приложении 7.

Пример схемы поверхности атаки



Блок №3. Поверхность атаки

Проблемы

- анализ интерпретаторов важен. Однако текст действующей версии Методики ВУ и НДВ, если трактовать его буквально, требует выполнять даже анализ тех интерпретаторов в составе СЗИ, которые объективно не составляют поверхность атаки

Подходы к решению

- улучшить текст таким образом, чтобы «буква закона» явно соответствовала его «духу»

Прототип решения

2. Требуется включить в состав модулей поверхности атаки и подвергнуть испытаниям в соответствии с уровнем контроля компоненты среды функционирования (а именно: виртуальная машина, библиотеки поддержки времени выполнения и стандартные библиотеки в составе виртуальной машины) интерпретируемых языков или языков, компилируемых в промежуточное представление, при наличии в составе поверхности атаки ОО модулей, написанных на указанных языках программирования. Допускается не проводить испытания в отношении данных компонент в случае фиксации в эксплуатационной документации ОО требования использования версий компонент (в объеме требований пункта 2.4.«з» настоящей Методики), ранее прошедших испытания по соответствующему или более высокому уровню контроля, , и выполнения остальных видов испытаний ОО с использованием указанных версий компонент.

Блок №4. Некоторые технологические аспекты

Блок №4. Некоторые технологические аспекты

Проблемы

- эффективных статических анализаторов для asm не известно, однако в действующей редакции Методики ВУ и НДВ отсутствие требования о необходимости статического анализа asm записано неявно, что регулярно порождало коллизии трактовки

- аналогично спорным является вопрос об эффективности статического анализа с точки зрения выявления угроз безопасности в отношении языков разметки

Подходы к решению

- явно прописать отсутствие необходимости статического анализа исходных asm-кодов

- явно прописать отсутствие необходимости статического анализа исходных кодов на языках разметки

Прототип решения

исходного текста на уровне синтаксического дерева. Не требуется проведение статического анализа исходных текстов, написанных на языках разметки (в частности: html, css3, xaml и т.п.). Не требуется проведение статического анализа исходных текстов, написанных на различных ассемблерах.

Блок №4. Некоторые технологические аспекты

Проблемы

- защищенность информации состоит из целостности, конфиденциальности и доступности информации. Традиционно о доступности любят забывать

Подходы к решению

- в соответствии с тем, что ФСТЭК России всё больше акцентирует внимание на качественных характеристиках СЗИ, в том числе в новых Требованиях к NGFW и СУБД, в явном виде вводить требования к проверке обеспечения доступности информации

Прототип решения

4.1.2.4. Дополнительные требования к исследованиям (усиления)

1. Требуется выполнить автоматизированный динамический анализ, направленный на подтверждение устойчивости СЗИ к специфическим угрозам, характерным для данного типа СЗИ, определяемым испытательной лабораторией совместно с разработчиком (как например: … , устойчивость системы к DDoS-атакам, … и т.п.).

Блок №4. Некоторые технологические аспекты

Проблемы

- в действующей редакции Методики ВУ и НДВ специфическому анализу WEB-интерфейсов уделялось недостаточно внимания

Подходы к решению

- усилить и конкретизировать направление анализа WEB-интерфейсов

Прототип решения

4.1.2.3.70. Требуется выполнить анализ выявленных веб-интерфейсов, составляющих поверхность атаки статическими методами, на предмет наличия уязвимостей, в объеме не менее чем 10ти основных пунктов и составляющих их подпунктов актуальной на момент испытаний редакции списка OWASP Top 10.

3. Требуется выполнить анализ мобильного браузерного кода (JavaScript, ActiveX, WebAssembly и т. п.) на предмет наличия потенциально опасных функциональных возможностей, НДВ и известных уязвимостей с использованием автоматизированных средств анализа, либо в соответствии с требованиями

В отношении фаззинга web-приложений с помощью web-фаззеров:

- веб-приложений посредством анализа кодов возврата и иных параметров ответов веб-приложений на формируемые фаззером запросы.

ФАЗЗИНГ – раздел увеличился в размерах за счёт более детального описания требуемых активностей.

Эксперту следует ориентироваться на уровень технологической зрелости, позволяющий получить оценку не ниже «хорошо с плюсом» на курсах по фаззингу ФСТЭК России на базе ИСП РАН

Блок №4. Некоторые технологические аспекты

Проблемы

- анализ утечек помеченных данных до сих пор пытаются выполнять средствами usermode-уровня, такими как valgrind/callgrind

- анализ утечек помеченных данных до сих пор пытаются выполнять методами «вставки датчиков» в исходный код тестируемого приложения

Подходы к решению

- ещё более явно зафиксировать, что анализ утечек помеченных данных следует выполнять в режиме полносистемной эмуляции

Прототип решения

пользователем через графический, консольный или файловый интерфейс. Не допускается выполнение анализа помеченных данных методом статической инструментации (вставка датчиков) исходных текстов ОО, либо инструментами анализа помеченных данных пользовательского режима.

Блок №5. Распределение обязанностей и Центры компетенций

Блок №5. Распределение обязанностей и Центры компетенций

Проблемы

- мартышкин труд – в ходе сотен идущих испытаний выполняются сотни одинаковых анализов одного и того же компонента (частный пример – анализ nginx, который входит в состав каждого третьего СЗИ)

- низкое качество испытаний – отсутствует обмен опытом и менторская поддержка по конкретному анализируемому компоненту

- выполнение анализа сторонних компонентов в полном объеме как правило нереализуемо силами одной организации-разработчика за время одной итерации испытаний

Подходы к решению

- стимулировать совместную работу над наиболее важными сторонними компонентами под эгидой Центров Компетенций ФСТЭК России

- учитывать итеративный вклад разработчика в исследование компонента в качестве кванта работы, достаточного для прохождения итерации испытаний

Блок №5. Распределение обязанностей и Центры компетенций

Прототип решения

3. Требуется выполнить статический анализ исходных текстов, разметку и исправление подтвержденных уязвимостей заимствованных модулей составляющих поверхность атаки в объеме, не меньшем чем объем зафиксированный в типовых методиках исследования данного вида модулей, рекомендуемых ФСТЭК России. В ходе исследований должна применяться типовая методика в редакции, действующей на момент подачи заявки на проведение сертификационных испытаний;

3. Требуется выполнить фаззинг-тестирование составляющих поверхность атаки заимствованных модулей и исправление подтвержденных уязвимостей в объеме, не меньшем чем объем зафиксированный в типовых методиках исследования данного вида модулей, рекомендуемых ФСТЭК России. В ходе исследований должна применяться типовая методика в редакции, действующей на момент подачи заявки на проведение сертификационных испытаний;

Блок №5. Распределение обязанностей и Центры компетенций

Проблемы

- в ряде случаев эксперты не обладают знаниями и опытом для выполнения Методики ВУ и НДВ в отношении ОО, однако при этом в ходе испытаний – при том, что договор на испытания уже заключен – полностью возлагают ответственность за проведение всех испытаний на разработчика, ставя выдачу положительного Технического заключение в прямую зависимость от успешности его работы, и фактически устраняются от проведения испытаний

Подходы к решению

- обезопасить разработчика от взаимодействия с неквалифицированным экспертом – явно обязать эксперта выполнять конкретные блоки работ в ходе сертификационных испытаний

Блок №5. Распределение обязанностей и Центры компетенций

Прототип решения

сертификационных испытаний. Дополнительно испытательной лаборатории требуется:

- верифицировать разметку предупреждений, классифицированных разработчиком как:
  - «верные, не требующие исправления», в первую очередь;
  - «ложноположительные», во вторую очередь;

в отношении не менее чем 100 предупреждений для каждого из использованных статических анализаторов, начиная с предупреждений высшего уровня критичности и далее в порядке снижения степени критичности.

Объем и результаты выполненных испытательной лабораторий исследований фиксируются в протоколе испытаний.

сертификационных испытаний. Дополнительно испытательной лаборатории требуется:

- сформировать и передать разработчику не менее одного дополнительного фаззинг-теста для каждого модуля, составляющего поверхность атаки, либо значимо улучшить существующий комплект фаззинг-тестов модуля (например: улучшить коллекцию, расширить словарь, добавить датчик срабатывания ошибок и т.п). Фаззинг-тест должен быть сформирован в парадигме тестирования, уже применяемой разработчиком. При выборе подлежащего тестированию участка кода следует анализировать участки, наиболее значимые для безопасности ОО.

Объем и результаты выполненных испытательной лабораторий исследований фиксируются в протоколе испытаний.

Коммуникационные ресурсы сообщества под эгидой Центра компетенций ФСТЭК России и ИСП РАН

Благодарю за внимание!

Дмитрий Пономарев

технический директор **ООО НТЦ «Фобос-НТ»**
сотрудник **ИСП РАН**

@DmitryJustDmitry