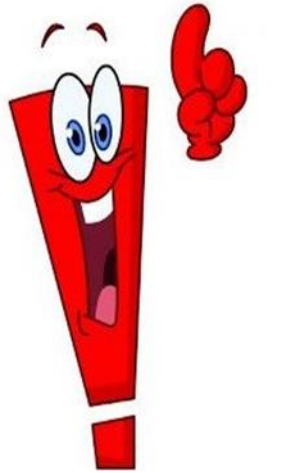
О снижении рисков атак, использующих программные закладки и уязвимости в проектах с открытым исходным кодом

Владимир Комисаренко,
заместитель директора по проектам в сфере защиты информации

Проблематика



- Проблема давно существующая
- Санкции
- Особенно обострилась на фоне военно-политической ситуации
- В гражданской сфере (банки и иные важные системы)
- Стала частью противостояния

В Республике Беларусь

УТВЕРЖДАЮ

Председатель Правления
Национального банка
Республики Беларусь

_____ П.В.Каллаур

«26» июня 2020 г.

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ И ПРАВИЛА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Информационные технологии и безопасность
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
БАНКОВ РЕСПУБЛИКИ БЕЛАРУСЬ
Требования к системам менеджмента информационной безопасности**

ТТП ИБ 2.1-2020

21.33 Для программных компонентов АБС, реализующих банковский платежный технологический процесс или предназначенных для обработки персональных данных, данных держателей платежных карточек или иной информации, в отношении которой законодательством Республики Беларусь, международным законодательством или решением организации БС установлено требование об обеспечении безопасности, рекомендуется перед проведением предварительных испытаний осуществлять контроль исходного кода с целью выявления типовых ошибок программирования и иных дефектов, приводящих к возникновению уязвимостей.

В Российской Федерации

Программная закладка: Преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения.
Примечание - Программная закладка может быть реализована в виде вредоносной программы или программного кода

Недекларированные возможности (программного обеспечения): Функциональные возможности программного обеспечения, не описанные в документации.

Контроль исходного кода

ТТП ИБ 2.1 – 2020

Приложение Г

РЕКОМЕНДАЦИИ К ПРОВЕДЕНИЮ КОНТРОЛЯ ИСХОДНОГО КОДА

1. Общие положения

1.1. Контроль кода (codereview) - мероприятия, осуществляемые в отношении определенных частей исходного текста (исходного кода) программы для ЭВМ, созданных одним или несколькими разработчиками, другим (не создававшим эту часть кодов) разработчиком или назначенным в установленном порядке иным имеющим требуемую подготовку специалистом, и которые состоят в детальной проверке (изучении, анализе, исследовании) соответствующих исходных кодов с целью выявления неизвестных уязвимостей, в том числе связанных с ошибками программирования, нарушений установленных требований, а также иных существенных дефектов.

1.2. Объектом исследования являются тексты программ разрабатываемых компонентов АБС, в первую очередь тексты программ специализированных банковских приложений.

1.3. Контроль кода может в обоснованных случаях проводиться несколькими лицами, в том числе при участии создавшего и (или) модифицировавшего проверяемый код разработчика.

1.4. Контроль кода может осуществляться лицом, проверяющим код, как вручную, в том числе с использованием приемов эффективного чтения программного кода (codereading), так и с применением методов и средств автоматизированного анализа исходного кода, в том числе обеспечивающих:

– статический анализ кода;

– динамический анализ кода.

Основные типы уязвимостей

1. Не обнаруженные
1.1. Программные закладки. Функциональные закладки, участки кода способные выполнить действия не описанные в документации к ПО.
1.2. Участки кода, влияющие на процесс компиляции, снижая уровень проверки и/или отключающие информирование при сборке.
1.3. Переполнения буфера
1.4. Не обнаруженные и находящиеся в исполняемом коде при отсутствии соответствующего исходного (программные закладки).
2. Обнаруженные
2.1. Потенциальные угрозы, информация о которых обнаружена среди обращений пользователей, через список рассылки .
2.2. Классифицированные, но не устраненные – стоят в списке на устранение зафиксированные как планируемые исправления.
2.3. Классифицированные, устраненные – зафиксированные как уязвимости в базе данных CVE, самого программного обеспечения и его зависимостей.

Наши преимущества

- Наша методология направлена на снижение рисков, связанных с указанными выше проблемами
- Делаем как для себя

Тестирование на проникновение

- Пентестинг (методологии: черный, серый, белый ящики)
- Специализированные сервисы типа Hackerone
- Расценки за результат, багбаунти
- Инициативы компаний (багбаунти)
- Можно ли доверять или в какой степени?
- Отключены российские ресурсы
- Выброшены российские хакеры
- Баланс между честностью и суммой бонуса (в отношении НДВ)

Отечественные сервисы

- Аналогичные сервисы в России и Беларуси
- Отечественная сборка – уже хорошо! – сильно уменьшает риск НДВ
- Заимствованные компоненты исходного кода и внешние модули
- Риски сотрудничества с open source проектами (пример Baikal)

Действия. Поиск и правильная сборка

- Определить доверенный исходный код. Организация получения исходного кода с трех различных ip адресов (например, принадлежащих различным странам)

- Осуществление сборки исходного кода с использованием собственной системы управления версиями зафиксированной и изолированной от сети интернет

Обновления

Выбор / определение версии для обновления:

- анализ информации из рассылки на предмет поиска выявленных ошибок в новых версиях
- анализ внесенных изменений, согласно списку внесенных изменений в исходный код
- принятие решения обновлять или нет в зависимости от внесенных изменений

Безопасность

Если обновлять, то оценка безопасности того, что привнесено:

- построение покрытия тестовыми наборами путем тестирования
- ручной анализ не покрытых участков кода на предмет не документированного и подозрительного функционала
- проведение анализа исхода кода несколькими анализаторами
- анализ результатов статических анализаторов на предмет ложных срабатываний

Поиск функциональных закладок

Поиск функциональных закладок в исходном тексте с использование ПО собственной разработки:

- Не имеет «бомб отложенного действия» (Does not have time bombs or other time-based attacks). Имеющих пассивный алгоритм активации (наступление определенного временного интервала, достижение определенного размера используемых файлов)
- Не «звонит домой» (Does not "phone home" to malicious or unauthorized destinations). Активный алгоритм активации (получение определенного набора данных по сетевым протоколам, регистрация имени пользователя с ожидаемыми характеристиками)
- В нём нет лазеек, «пасхальных яиц», атак «салями», руткитов или несанкционированного кода, которым может управлять злоумышленник. Does not have back doors, Easter eggs, salami attacks, rootkits, or unauthorized code that can be controlled by an attacker

Меры, направленные на снижение угроз

- проводить анализ необходимости использования дополнительных мер защиты на основании планируемых изменений (К примеру, https://commitfest.postgresql.org) и списка рассылки безопасности (https://lists.postgresql.org)
- осуществлять компиляцию исходного кода с настройками, исключающими и/или затрудняющими использование класса уязвимостей переполнение буфера
- направление запросов разработчику для формализации выявленных подозрительных участков кода и/или их исправления

Меры, направленные на снижение угроз

- Анализ результатов сканирования ИС, к которой используется рассматриваемое ПО. Анализ отчетов. Рекомендации по закрытию выявленных уязвимостей, либо по недопущению их эксплуатации
- Анализ имеющейся в отчетах информацию о небезопасных настройках в ИС и рекомендации по их устранению (недопущению эксплуатации)
- На выходе: заключение и рекомендации по установке ПО в промышленную среду

Криптографическое ПО

Опробовали эту методологию в том числе на криптографическом ПО. Как правило считается, что это ПО сильно проверено. Однако, объем его кода велик, много заимствований на уровне как исходного кода, так и вызываемых модулей. НДВ найти не удалось. Но удалось найти проблемы в коде. Работа идет и в настоящее время

LWO

В ритме инноваций

lwo.by
contact@lwo.by
+375 17 334 10 02
+375 17 334 28 27
ул. Кропоткина, д. 91, Минск
Республика Беларусь, 220002