Отчет о результатах проверки корректности устранения уязвимостей стенда на базе банкомата NCR selfserv 22  
АКБ "РосЕвроБанк" (ОАО)

Москва, 2015

Оглавление

[Оглавление 2](#_Toc430352843)

[Обозначения и сокращения 3](#_Toc430352844)

[1. Введение 4](#_Toc430352845)

[1.1. Общие сведения 4](#_Toc430352846)

[1.2. Цели проведения работ 4](#_Toc430352847)

[1.3. Описание проекта 4](#_Toc430352848)

[2. Методика проведения работ 5](#_Toc430352849)

[2.1. Условия и порядок проведения работ 5](#_Toc430352850)

[2.2. Модель нарушителя 5](#_Toc430352851)

[2.3. Оценка уровня критичности уязвимостей 6](#_Toc430352852)

[3. Описание объекта исследования 7](#_Toc430352853)

[4. Результаты работ 9](#_Toc430352854)

[5. Результаты проверки устранения уязвимостей 12](#_Toc430352855)

[6. Инструментальное сканирование Системы 17](#_Toc430352856)

[Приложение А. Реестр уязвимостей 23](#_Toc430352857)

[Приложение Б. Перечень установленного ПО 33](#_Toc430352858)

# Обозначения и сокращения

|  |  |  |
| --- | --- | --- |
| NDC | – | NCR Direct Connect – прикладной протокол передачи данных, используемый в банкоматах |
| PAN | – | Primary account number – номер платежной карты |
| Track2 (или трек) | – | Вторая дорожка магнитной полосы банковской карты. На дорожке содержится номер карты, срок действия и различная сервисная информация |
| XFS (или CEN/XFS) | – | eXtensions for Financial Services – стандарт и программная реализация интерфейса между периферийными устройствами и прикладным ПО для банкоматов на платформе Windows. Описывает взаимодействие со всеми входящими в банкомат устройствами независимо от производителя |
| Диспенсер | – | Устройство выдачи банкнот в банкомате |
| Кардридер | – | Устройство для чтения/записи информации магнитной полосы, а также для взаимодействия с чипом платежных карт |
| ЛВС | – | Локальная вычислительная сеть |
| ОС | – | Операционная система |
| Пинпад | – | Устройство ввода цифровой информации в банкомат, в том числе пин-кода, ключей шифрования |
| ПО | – | Программное обеспечение |

# Введение

## Общие сведения

Настоящий документ разработан в соответствии с договором №054-14/ПТ/С от 4 декабря 2014 года, заключенным между АКБ «РосЕвроБанк» (ОАО) (далее – Заказчик) и ЗАО «Позитивные Технологии» (далее – Исполнитель) и содержит описание проверки корректности устранения уязвимостей, выявленных в результате анализа защищенности банкомата Заказчика. В ходе проекта специалисты Исполнителя провели исследование и инструментальное сканирование двух предоставленных Заказчиком банкоматов, а также анализ защищенности программного и программно-аппаратного обеспечения банкоматов (далее – Система). Работы проводились в период с «21» июля по «28» июля 2015 года.

Данный документ содержит подробное описание хода и результатов работ по проверке корректности устранения уязвимостей, выявленных в результате анализа защищенности стенда с набором устройств на базе банкомата NCR SelfServ 22.

## Цели проведения работ

Целью работ является получение независимой оценки текущего состояния информационной безопасности Системы путем выявления существующих уязвимостей, которые не были устранены по результатам анализа защищенности Системы Заказчика, проведенного ранее.

## Описание проекта

В рамках работ проводились:

1. Исследование и инструментальное сканирование Системы;
2. Проверка устранения уязвимостей программного и программно-аппаратного обеспечения Системы, выявленных в рамках проведенного ранее анализа защищенности.

Работы по анализу защищенности Системы осуществлялись на территории Заказчика.

Для проведения инструментального сканирования оборудования Системы Исполнитель провел адаптацию ПО, которая осуществлялась на территории Исполнителя. Разработка специализированного ПО для демонстрации атак также осуществлялась на территории Исполнителя.

Отладка разрабатываемых специализированных проверок проводилась на анализируемой Системе на территории представителя Заказчика.

Методика проведения работ описана в разделе 2. Описание объекта исследования приведено в разделе 3. Основные результаты работ приведены в разделе 4. Описание результатов проверки устранения уязвимостей приведено в разделе 5 настоящего документа. Результаты инструментального сканирования приведены в разделе 6. Перечень выявленных уязвимостей представлен в приложении А к настоящему документу. Полный перечень установленного в Система ПО приведен в приложении Б к настоящему документу.

# Методика проведения работ

## Условия и порядок проведения работ

Специалистам Исполнителя был предоставлен непосредственный физический доступ к банкомату (с возможностью доступа в сервисную зону банкомата), а также с возможностью отладки используемого в ходе работ ПО на территории представителя Заказчика.

Специалисты Исполнителя провели предварительный аудит Системы на территории Заказчика, в задачи которого входило выявление:

* основных компонентов Системы;
* версий программного и аппаратного обеспечения;
* особенностей сетевого взаимодействия;
* используемых протоколов передачи данных.

На основании проведенного аудита специалисты Исполнителя провели адаптацию специализированного ПО (базы знаний системы MaxPatrol) для осуществления автоматизированных проверок на оборудовании Заказчика.

Инструментальное сканирование проводилось с помощью автоматизированной системы поиска уязвимостей и проверки соответствия стандартам MaxPatrol в режиме системного сканирования (Audit).

Для проверки корректности устранения выявленных ранее уязвимостей в Системе использовалась комбинация инструментальных методов анализа и ручного исследования компонентов Системы экспертами. В рамках работ было проверено наличие или отсутствие в Системе всех уязвимостей, выявленных при анализе защищенности, который был проведен в рамках предыдущего проекта.

## Модель нарушителя

В рамках работ осуществлялось моделирование действий потенциального злоумышленника, относящегося к следующим категориям:

* Внешний нарушитель, обладающий физическим доступом к Системе, но не обладающий никакими предварительными сведениями о Системе и логическим доступом к Системе (за исключением общедоступных интерфейсов);
* Внешний или внутренний нарушитель, обладающий логическим доступом к сети, к которой подключена Система (например, администратор ЛВС Заказчика, администраторы провайдера, а также внешний нарушитель, обладающий физическим доступом к кабелю Ethernet банкомата);
* Внешний или внутренний нарушитель, обладающий физическим доступом к Системе, в том числе доступом в сервисную зону банкомата (включая системный блок, интерфейсы USB, Ethernet), но не имеющий иного логического доступа к Системе (например, инкассаторы, сервис-инженеры, техники, а также внешний нарушитель, обладающий копией ключа сервисной зоны).

## Оценка уровня критичности уязвимостей

По результатам тестирования каждой из выявленных уязвимостей присваивается определенный уровень критичности в зависимости от степени воздействия на уязвимый ресурс и в зависимости от сложности эксплуатации данной уязвимости. Уровень риска для уязвимостей выставляется экспертами Исполнителя по качественной шкале: Высокий/Средний/Низкий.

В качестве основного критерия для оценки уровня риска и сложности эксплуатации уязвимости используется международная система оценки уязвимостей Common Vulnerability Scoring System (CVSS) v2.0 в части базовых метрик.

Базовые метрики CVSS включаю в себя следующие группы метрик:

Метрики оценки сложности эксплуатации, которые оценивают, как получить доступ к уязвимости и нужны ли для эксплуатации уязвимости дополнительные условия:

* AccessVector (Вектор доступа);
* Access Complexity (Сложность доступа);
* Authentication (Аутентификация)

Метрики воздействия, которые описывают возможное прямое влияние на IT-систему в случае эксплуатации уязвимости:

* Confidentiality Impact (Влияние на конфиденциальность);
* Integrity Impact (Влияние на целостность);
* Availability Impact (Влияние на доступность).

При этом влияние на систему определяется независимо для свойств конфиденциальности, целостности и доступности.

Для каждой уязвимости определяется значение соответствующих метрик, и эти значения указываются в качестве вектора. Каждая метрика в этом векторе представлена сокращенным именем метрики, за которым следует ":" (двоеточие), а затем – сокращенное значение метрики. Вектор содержит последовательность метрик в заранее заданном порядке, при этом символ "/" используется для разделения метрик.

Базовый вектор CVSS имеет следующий формат:

AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]

В зависимости от значений метрик для уязвимости рассчитывается общая оценка уровня риска от 0 до 10.

Качественная оценка уровня риска присваивается на основе количественной оценки CVSS следующим образом:

* Оценка CVSS от 0 до 4 соответствует низкому уровню риска;
* Оценка CVSS от 4 до 6,9 соответствует среднему уровню риска;
* Оценка CVSS от 7 до 10 соответствует высокому уровню риска.

Качественная оценка сложности эксплуатации также оценивается на базе метрик сложности эксплуатации CVSS.

В связи с тем, что методика CVSS является универсальной и может не учитывать особенности конкретных систем, в ряде случаев специалисты Исполнителя корректируют качественные оценки риска и сложности эксплуатации на основе своего экспертного мнения.

# Описание объекта исследования

В границы проведения работ входит банкомат NCR SelfServ 22 с ОС Windows XP Pro Service Pack 3 и набором ПО. Перечень установленного ПО представлен в приложении Б.

Исследуемая Система – тестовый стенд, соответствующий реально используемым банкоматам Заказчика по составу программного и программно-аппаратного обеспечения. При этом рассмотренная в рамках данного исследования Система отличается по составу программного и программно-аппаратного обеспечения от исследованной в рамках анализа защищенности, который был проведен в рамках предыдущего проекта.

Для проведения работ представителем Заказчика (компанией «Банком») была сформирована тестовая лаборатория. Настройки Системы были установлены в соответствии с применяемыми у Заказчика требованиями информационной безопасности к системам данного типа, обновленными с учетом рекомендаций, подготовленных специалистами Исполнителя по результатам анализа защищенности банкомата NCR SelfServ 32. В состав стенда также было включено соединение с тестовым процессинговым центром (БПЦ). Полный список установленного ПО представлен в прилагаемом отчете системы MaxPatrol.

Анализ привнесенного аппаратного обеспечения, не связанный напрямую с выявленными ранее уязвимостями, не входит в границы работ.

Система состоит из системного блока банкомата и периферийных устройств, подключенных к нему через USB-интерфейсы (диспенсер, кардридер, пинпад, сенсоры). Системный блок подключен к процессинговому центру банковской системы (Процессинг).

Подключение к процессинговому центру может осуществляться одним из трех способов (см. Рисунок 1):

* **С использованием программного VPN-клиента.** В качестве программного VPN-клиента может быть использовано ПО OpenVPN Client либо Cisco VPN Client. Программный VPN-клиент устанавливается в Системе и осуществляет подключение к процессинговому центру через арендованные каналы связи.
* **С использованием аппаратного VPN-клиента**. Аппаратный VPN-клиент устанавливается в непосредственной близости от Системы и обеспечивает подключение Системы к процессинговому центру через арендованные каналы связи.
* **Прямым подключением** через арендованные каналы связи.



Рисунок . Типовая конфигурация Системы

В рамках проведенного исследования в тестовой среде было реализовано прямое подключение к процессинговому центру.

# Результаты работ

В результате проведения проверки корректности устранения Заказчиком выявленных в системе уязвимостей были получены следующие основные результаты:

* **Выявлены возможности выхода из режима киоска, реализации атак с целью несанкционированной выдачи банкнот, перехвата чувствительных данных (Track2) и реализации атак на ОС банкомата**, в следствие эксплуатации не устранённых Заказчиком уязвимостей. Большая часть уязвимостей (52,4% от общего числа) были устранены Заказчиком, что подтверждает проведенная проверка. При этом почти половина (47,6% от общего числа) уязвимостей не были устранены. Данная статистика, предположительно, вызвана тем, что для проведения работ по проверке устранения уязвимостей Заказчиком была предоставлена система, отличная по составу программного и программно-аппаратного обеспечения от системы, рассмотренной в рамках предыдущего проекта. Доля устраненных и не устраненных уязвимостей представлена на диаграмме ниже (см. Рисунок 2). Подробные результаты проверки устранения уязвимостей представлены в разделе 5 в Таблица 2.

Выявленные уязвимости позволяют нарушителю подменять процессинговый центр, проводить атаки с целью несанкционированной выдачи банкнот, перехватывать чувствительную информацию в результате реализации атаки «Человек посередине». Также существует потенциальная возможность несанкционированной выдачи банкнот в результате реализации атак на ОС систему банкомата.

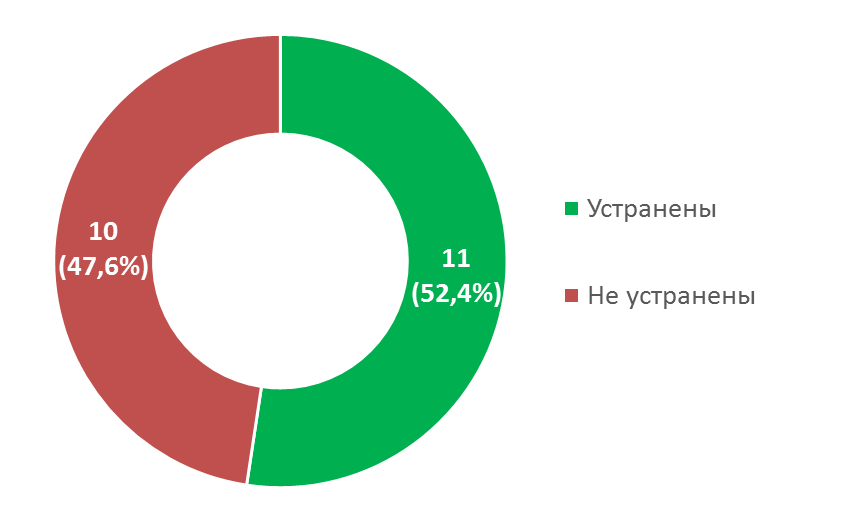


Рисунок . Доля устраненных и не устранённых уязвимостей

* **Выявлено 39 критических уязвимостей, 8 уязвимостей средней степени риска** в результате инструментального сканирования Системы. Ряд выявленных уязвимостей не был устранен Заказчиком, в частности не была установлена актуальная версия ОС. Также не были устранены уязвимости, связанные с недостатками парольной политики. Был выявлен ряд новых уязвимостей, в частности критические уязвимости в Microsoft .NET Framework версий 1.1 SP1 и 2.0 SP2. Это связано с тем, что в рамках проведения данного исследования работы проводились в отношении Системы, отличающейся по составу ПО от Системы, рассматриваемой в рамках проекта по анализу защищенности, проведенного ранее. Важно отметить, что специалисты Заказчика устранили большинство уязвимостей, выявленных в рамках анализа защищенности. При этом не устранённые Заказчиком критические уязвимости позволяют нарушителю осуществлять атаки на Систему, в том числе получить полный контроль над Системой или полностью вывести ее из строя. Для реализации атак нарушителю необходим физический доступ к сервисной зоне банкомата, а также доступ к ОС.

В таблице ниже приведена оценка защищенности банкомата по отношению к атакам от различных категорий нарушителей в результате устранения выявленных ранее уязвимостей.

Таблица . Оценка защищенности банкомата по отношению к атакам от различных категорий нарушителей

|  |  |  |  |
| --- | --- | --- | --- |
| **Параметр** | **До устранения уязвимостей** | **В результате устранения уязвимостей** | **краткое Описание** |
| **Уровень защищенности банкомата от злоумышленника, обладающего только физическим доступом к банкомату (без доступа к сервисной зоне)** – при подключении банкомата к процессинговому центру через аппаратный VPN-клиент, размещаемый в пределах сервисной зоны | **Приемлемый** | **Приемлемый** | В рамках проведения работ не выявлено уязвимостей, позволяющих проводить атаки на банкомат со стороны данного типа нарушителя. |
| **Уровень защищенности банкомата от злоумышленника, обладающего только физическим доступом к банкомату (без доступа к сервисной зоне)** – при подключении банкомата к процессинговому центру напрямую, либо через программный VPN-клиент, либо через аппаратный VPN-клиент, размещаемый вне сервисной зоны | **Крайне низкий** | **Низкий** | В результате устранения уязвимостей специалисты Заказчика не обеспечили добавление MAC-значений в транзакционные запросы и ответы, что позволяет нарушителю проводить атаки с целью несанкционированной выдачи банкнот. Уязвимости, связанные с отсутствием шифрования данных на прикладном уровне (NDC), а также с возможностью проведения атак ARP Poisoning, не были устранены Заказчиком. Существует возможность перехвата значений Track2 (см. Рисунок 3).  Подключение к процессинговому центру осуществляется напрямую по незащищенному каналу связи, что позволяет нарушителю (при отсутствии MAC-значений в транзакционных запросах и ответах) подменить процессинговый центр и осуществить атаки с целью несанкционированной выдачи денежных средств. |
| **Уровень защищенности банкомата от злоумышленника, обладающего доступом к сети банкомата** | **Крайне низкий** | **Низкий** | В результате работ выявлено, что уязвимости, позволяющие осуществить подмену процессингового центра не были устранены. Возможны атаки с целью несанкционированной выдачи денежных средств. Существует возможность перехвата значений Track2 (см. Рисунок 3).  Возможно проведение атак на ОС устаревшей версии, которая не поддерживается производителем, и для атак на которую существует множество общедоступных эксплойтов. Потенциально, реализация таких атак может привести к несанкционированной выдаче банкнот.  Отсутствие системы контроля целостности позволяет нарушителю проводить атаки и выполнять произвольный код в системе.  Недостаточная защита взаимодействия ОС с периферийными устройствами позволяет нарушителю проводить атаки, направленные на несанкционированную выдачу денежных средств. |
| **Уровень защищенности банкомата от злоумышленника, обладающего физическим доступом в сервисную зону** | **Крайне низкий** | **Низкий** | В результате работ по устранению уязвимостей специалисты Заказчика установили стойкий пароль для доступа к BIOS, что не дает возможности нарушителю изменять настройки, при этом была выявлена возможность загрузки сторонней ОС с внешнего носителя (USB) без доступа к BIOS. Нарушитель может получить полный контроль над системой.  Также не была устранена уязвимость «Недостаточно эффективная защита от выхода из киоска KeyBoardDisabler», которая позволяет нарушителю получить доступ к ОС путем нажатия горячих клавиш на подключенной клавиатуре. |

# Результаты проверки устранения уязвимостей

Результаты проверки устранения уязвимостей представлены в таблице Таблица 2.

Таблица . Результаты проверки устранения уязвимостей

| **Уязвимость или недостаток механизма безопасности** | **Угроза** | **Результат проверки** |
| --- | --- | --- |
| Отсутствие аутентификации при доступе к BIOS | Загрузка ОС с внешних носителей, отключение механизмов защиты, выполнение произвольного кода в системе вплоть до несанкционированной выдачи денежных средств | Уязвимость устранена[[1]](#footnote-2) |
| Отсутствие аутентификации для входа в сервисный режим «Supervisor» | Несанкционированная выдача денежных средств | Уязвимость устранена |
| Выполнение произвольных команд в ПО Zytronic UPDD (Buffer Overflow) | Несанкционированный доступ к Системе с привилегиями приложения, несанкционированная выдача денежных средств | Уязвимость устранена[[2]](#footnote-3) |
| Использование устаревших версий прикладного ПО и ОС | Получение полного контроля над ОС банкомата, вплоть до несанкционированной выдачи денежных средств | Выявлена уязвимость |
| Выполнение произвольного кода в Internet Explorer (MS13-008) | Получение несанкционированного доступа к Системе с привилегиями текущего пользователя, выполнение произвольных команд вплоть до несанкционированной выдачи денежных средств | Уязвимость устранена |
| Отсутствие механизмов противодействия атакам ARP Cache Poisoning | Перехват сетевого трафика, отказ в обслуживании | Выявлена уязвимость |
| Отсутствие MAC-значения в транзакционных запросах и ответах | Модификация трафика, несанкционированная выдача денежных средств | Выявлена уязвимость |
| Отсутствие шифрования при взаимодействии между банкоматом и процессингом на прикладном уровне | Перехват сетевого трафика. Несанкционированная выдача денежных средств, раскрытие чувствительной информации, включая Track2 | Выявлена уязвимость |
| Раскрытие чувствительной информации платежных карт | Раскрытие чувствительной информации (Track2) | Выявлена уязвимость |
| Избыточные привилегии учетной записи приложения | Полный контроль над Системой, вплоть до возможности осуществлять несанкционированную выдачу денежных средств | Уязвимость устранена[[3]](#footnote-4) |
| Недостаточно надежная схема генерации симметричных ключей | Несанкционированная выдача денежных средств | Выявлена уязвимость |
| Отсутствие аутентификации и шифрования данных при обмене информацией с кардридером | Раскрытие чувствительной информации платежных карт | Выявлена уязвимость |
| Недостаточная защита взаимодействия с периферийными устройствами | Несанкционированная выдача денежных средств, раскрытие чувствительной информации платежных карт. | Выявлена уязвимость |
| Выход за пределы киоска в ПО Intellect | Несанкционированный доступ к функциям ОС | Уязвимость устранена[[4]](#footnote-5) |
| ПО McAfee Solidcore for APTRA не обеспечивает защиту от эксплуатации уязвимостей доверенного ПО | Получение полного контроля над системой. Несанкционированная выдача денежных средств, раскрытие чувствительной информации. | Уязвимость устранена[[5]](#footnote-6) |
| Недостаточно эффективная защита от выхода из киоска KeyBoardDisabler | Получение полного контроля над Системой, несанкционированная выдача денежных средств, раскрытие чувствительной информации. | Выявлена уязвимость |
| Слабая парольная политика | Получение несанкционированного доступа к ресурсам с правами соответствующего пользователя | Уязвимость устранена |
| Некорректная настройка списка доверенного ПО в ПО McAfee Solidcore for APTRA | Получение несанкционированного доступа к ресурсам | Уязвимость устранена[[6]](#footnote-7) |
| Недостаточная защита данных при их передаче между банкоматом и процессинговым центром | Раскрытие чувствительной информации. | Выявлена уязвимость |
| Использование ПО удаленного администрирования RAdmin | Несанкционированный доступ к ресурсу с привилегиями администратора. | Уязвимость устранена |
| Недостатки межсетевого экранирования | Проведение атак на Систему. | Уязвимость устранена |

Возможность перехвата значений Track2 продемонстрирована на Рисунок 3.

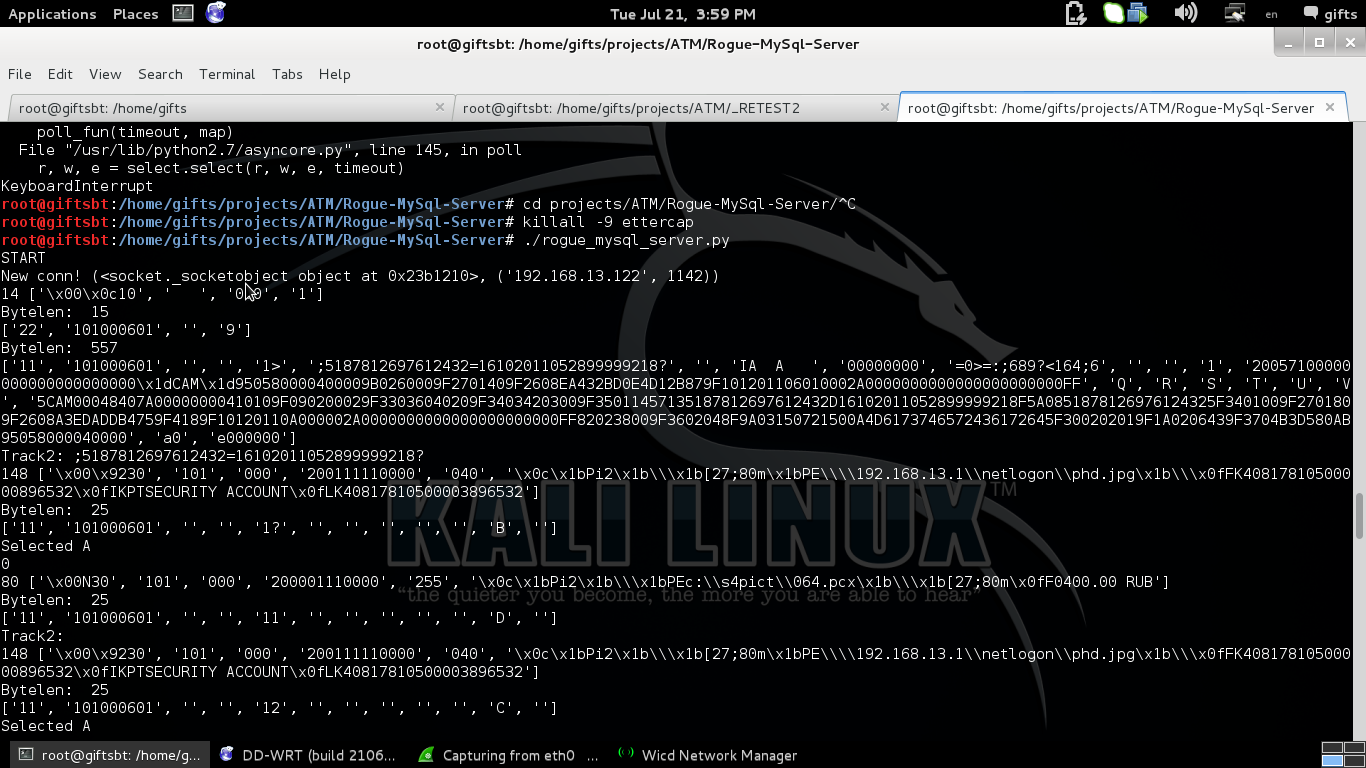


Рисунок . Перехват значений Track2

Настройка BIOS банкомата предусматривала загрузку только с жестких дисков. Однако, при использовании USB-накопителей, отформатированных как USB-HDD, система BIOS определяла такой накопитель как наиболее приоритетный из "жестких дисков" и осуществлял загрузку ОС с данного внешнего носителя (см. Рисунок 4 и Рисунок 5).

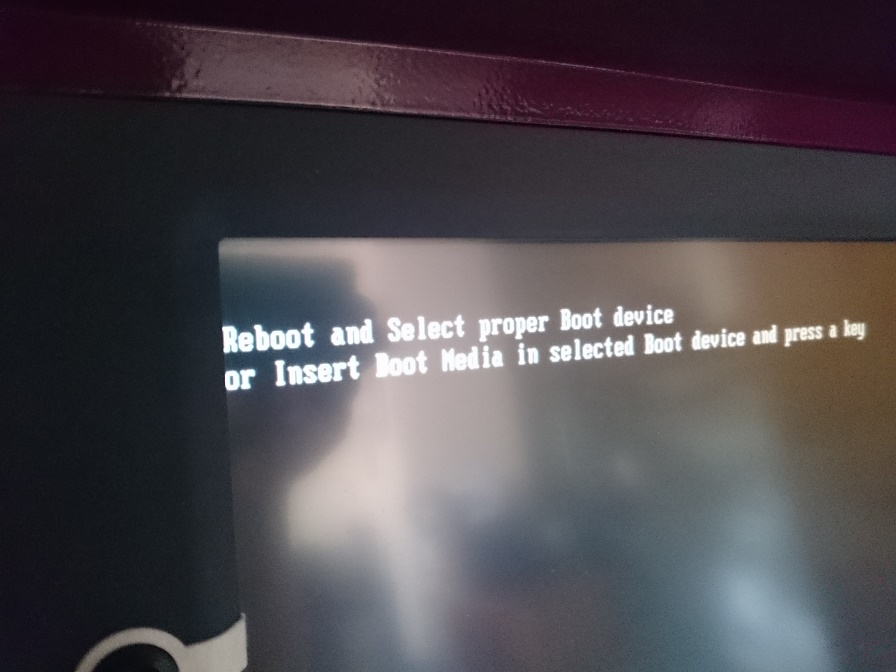
.

Рисунок . Загрузка с внешнего носителя без доступа к BIOS



Рисунок . Определение внешнего USB-накопителя как жесткого диска в системе BIOS

# Инструментальное сканирование Системы

Специалисты Исполнителя провели инструментальное сканирование Системы средствами автоматизированной системы анализа защищенности и контроля соответствия стандартам MaxPatrol в режиме белого ящика. База знаний системы MaxPatrol была предварительно адаптирована для поддержки специализированного ПО Системы Заказчика.

Основные результаты инструментального сканирования банкомата представлены в данном разделе. Отчеты системы MaxPatrol с детальным описанием обнаруженных уязвимостей и рекомендациями по их устранению прилагаются к данному отчету в электронном виде.

В результате сканирования было обнаружено в общей сложности 47 уязвимости различной степени риска (см. Рисунок 4). Среди них 39 уязвимостей (83% от общего количества) являются критическими и 8 (17% от общего количества) – средней степени риска.

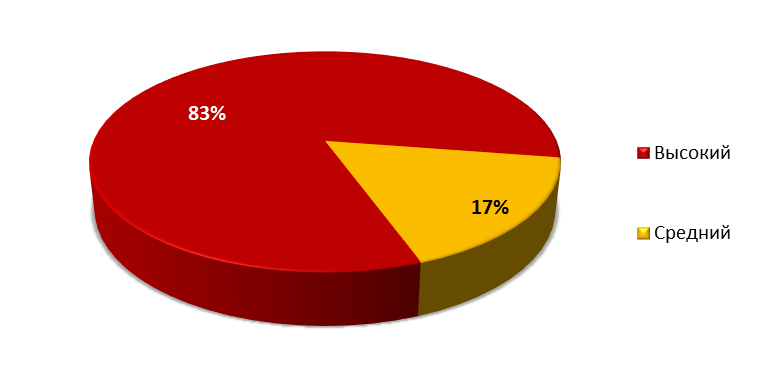


Рисунок . Доля выявленных уязвимостей различной степени риска

Проведенная проверка корректности устранения уязвимостей показывает, что в Системе устранено множество недостатков, выявленных ранее. Общее количество уязвимостей сократилось более, чем в 10 раз. Число критических уязвимостей снизилось с 430 до 39, а уязвимостей средней степени риска – с 118 до 8. Недостатков низкой критичности не было выявлено вовсе в рамках проведенной проверки. Диаграмма, отражающая количество выявленных уязвимостей до и после работ по их устранению, представлена на Рисунок 5.

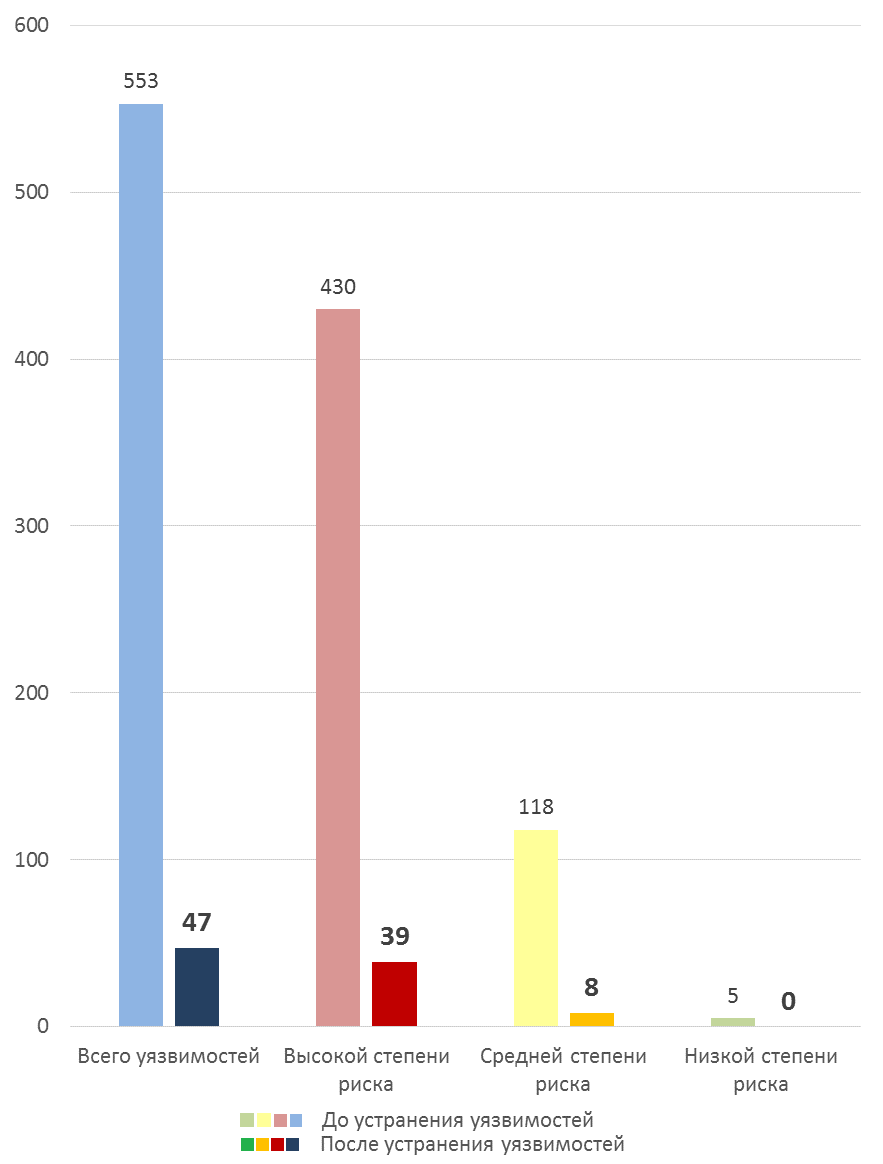


Рисунок . Количество выявленных уязвимостей до и после проведения работ по устранению уязвимостей (сравнительная диаграмма)

Таким образом, проведенное исследование показывает, что специалисты Заказчика устранили большинство уязвимостей в Системе. При этом в Системе выявлено значительное количество уязвимостей высокой степени риска, которые могу привести как к получению нарушителем полного контроля над Системой, так и к возможности проведения атак на отказ в обслуживании.

Все критические уязвимости связаны с применением в Системе Заказчика устаревшей версии ОС MS Windows XP, поддержка которой прекращена компанией Microsoft, а также устаревших версий прикладного ПО (например, Internet Explorer и др.). Для эксплуатации уязвимостей в таких системах выявлено 8 общедоступных эксплойтов, которые существенно упрощают задачу злоумышленника по проведению атак на Систему. Перечень доступных эксплойтов представлен в Таблица 3.

Таблица . Перечень общедоступных эксплойтов

| **CVE** | **Базовая оценка CVSS** | **Эксплойт** |
| --- | --- | --- |
| CVE-2008-4841 | 10 | Переполнение стека в конвертере текста WordPad Word 97  <http://www.exploit-db.com/exploits/6560> |
| CVE-2014-0257 | 9.3 | Уязвимость, связанная с обходом типов  https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/local/ms14\_009\_ie\_dfsvc.rb |
| CVE-2012-1535 | 9.3 | Выполнение произвольного кода  <https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/browser/adobe_flash_otf_font.rb> |
| CVE-2010-3147 | 9.3 | Уязвимость при загрузке библиотек  <http://www.exploit-db.com/exploits/14733> |
| CVE-2012-0163 | 9.3 | Уязвимость проверки параметров в .NET Framework  <http://www.exploit-db.com/exploits/18777> |
| CVE-2007-0042 | 7.8 | Уязвимость в ASP.NET, связанная с завершением нулевым байтом  <http://www.exploit-db.com/exploits/30281> |
| CVE-2007-3456 | 6.8 | Выполнение произвольного кода  <http://www.exploit-db.com/exploits/30288> |
| CVE-2010-3332 | 5.0 | Атака с применением криптографического оракула (padding oracle) в ASP.NET  <http://www.exploit-db.com/exploits/15213> |

Выявлен ряд эксплойтов, позволяющих использовать уязвимости прикладного ПО, которое установлено в Системе, но не предназначено для непосредственной работы банкомата, например:

* Выполнение произвольного кода в Adobe Flash Player (CVE-2007-3456);
* Выполнение произвольного кода в Adobe Flash Player (CVE-2012-1535);
* Использование после освобождения в Microsoft Internet Explorer ([CVE-2014-1776](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1776)).

Атака на прикладное ПО возможна в случае, когда злоумышленник имеет возможность запустить данное ПО, то есть имеет доступ к ОС банкомата в результате эксплуатации других уязвимостей.

Рекомендуется удалить из Системы все ПО, которое не предназначено для непосредственной работы банкомата. Если такое ПО невозможно удалить из Системы, необходимо использовать ПО контроля целостности, не внося непредназначенное для работы банкомата ПО в список доверенного.

Специалисты Исполнителя рекомендуют Заказчику осуществить переход на актуальные версии ОС, ПО АТМ и прикладного ПО. В случае невозможности такого перехода, Заказчику необходимо принять существующие риски, обеспечить информационную безопасность Системы другими методами и средствами. В частности, рекомендуется применять современные антивирусные решения, регулярно проводить аудит безопасности, использовать строгую парольную политику, обеспечить разграничение доступа к критичным системам, а также применять различные программно-аппаратные решения для обеспечения защиты банкомата как на уровне ОС, так и на сетевом и физическом уровнях.

В системе так же выявлены уязвимости средней степени риска, связанные с недостатками конфигурации. Такие уязвимости составили чуть более 4% от общего числа выявленных недостатков (см. Рисунок 6). В частности, выявлены недостатки конфигурации, связанные с неограниченными максимальными и минимальными сроками действия пароля пользователей ОС. Специалисты исполнителя рекомендуют установить максимальный срок действия пароля равный 30 календарным дням. Обеспечить строгую парольную политику.

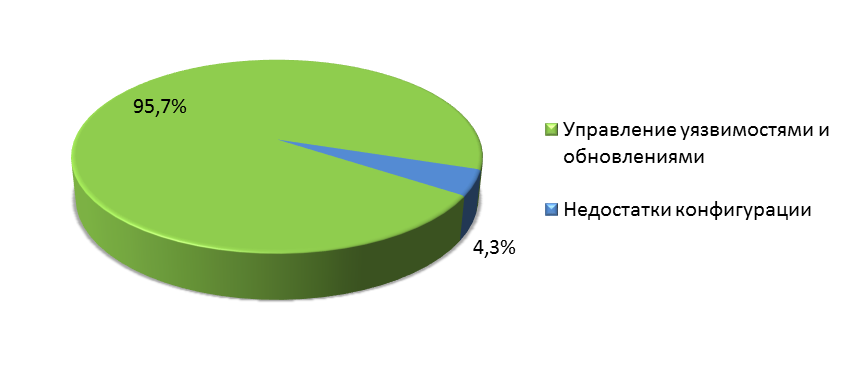


Рисунок . Доля выявленных уязвимостей различных категорий

Большинство уязвимостей были выявлены в рамках анализа защищенности Системы, проведенного в рамках предыдущего проекта до проведения Заказчиком работ по устранению уязвимостей. При этом в рамках проведенного исследования выявлен ряд новых уязвимостей, например, критические уязвимости в Microsoft .NET Framework версий 1.1 SP1 и 2.0 SP2, а также уязвимости средней критичности в Problem Determination Collection версии 2.07.0251, которые вызваны использованием устаревших версий ПО. Это связано с тем, что в рамках проведения проверки устранения выявленных уязвимостей работы проводились в отношении Системы, отличающейся по составу ПО от Системы, рассматриваемой в рамках проекта по анализу защищенности, проведенного ранее. Специалисты исполнителя рекомендуют устранить уязвимости, выявленные в данных компонентах Системы в соответствии с рекомендациями, приведенными в отчетах системы MaxPatrol.

|  |  |  |
| --- | --- | --- |
| **Уязвимость:**  Использование устаревших версий прикладного ПО и ОС | | |
| **Уровень риска: Высокий** | **CVSS: 7.9** (AV:A/AC:M/Au:N/C:С/I:С/A:С) | **Сложность:** Средняя |
| **Описание:**  В банкомате используется устаревшая версия ОС, для которой не осуществляется поддержка производителя. Также выявлено использование устаревших версий ПО. Злоумышленник может эксплуатировать уязвимости прикладного ПО и ОС, в том числе с применением общедоступных эксплойтов. | | |
| **Рекомендации:**  Необходимо удалить из Системы все ПО, которое не предназначено для работы банкомата. В случае невозможности удаления ПО (например, если прикладное ПО поставляется как неотъемлемый компонент ОС), следует использовать средства защиты, ограничивающие выполнение ПО.  Обновить используемые ОС и прикладное ПО до актуальных версий. В случае, если своевременная установка актуальных обновлений ПО и ОС невозможна, принять компенсационные меры, такие как регистрация и мониторинг событий безопасности. | | |
| **Уязвимость:**  Отсутствует ограничение на минимальный срок действия пароля | | |
| **Уровень риска: Средний** | **CVSS: 4** (AV:N/AC:H/Au:N/C:P/I:P/A:N) | **Сложность:** Высокая |
| **Описание:**  Обнаружено, что минимальный срок действия пароля неограничен. Подобная политика может привести к повторному использованию паролей пользователями.  Minimum password age = 0.  <http://technet.microsoft.com/en-us/library/cc779758.aspx> <http://www.microsoft.com/technet/security/prodtech/windows2000/w2kccadm/acctpol/w2kadm07.mspx> | | |
| **Рекомендации:**  Измените значение групповой политики на значение 1 или более дней (в соответствии с политикой безопасности, принятой в Вашей компании). Чтобы изменить ограничения на минимальный срок действия пароля, откройте Редактор групповых политик (Group Policy Editor) и выберите Конфигурация компьютера (Computer Configuration) - Конфигурация Windows (Windows Settings) - Параметры безопасности (Security Settings) - Политики учетных записей (Account Policies) - Политика паролей (Password Policy). Для внесения изменений дважды щелкните мышью на позиции "Мин. срок действия пароля" (Minimum password age), установите нужное значение в появившемся окне и нажмите "ОК". Изменения вступят в силу после применения групповой политики. | | |
| **Уязвимость:**  Слабое ограничение на срок действия пароля | | |
| **Уровень риска: Средний** | **CVSS: 4** (AV:N/AC:H/Au:N/C:P/I:P/A:N) | **Сложность:** Высокая |
| **Описание:**  Обнаружено, что максимальный срок действия пароля слишком велик или неограничен. Это может привести к успешным атакам подбора пароля.  Maximum password age = forever.  <http://technet.microsoft.com/en-us/library/cc736566.aspx> <http://www.microsoft.com/technet/security/prodtech/windows2000/w2kccadm/acctpol/w2kadm07.mspx> | | |
| **Рекомендации:**  Измените значение групповой политики на значение 30-60 дней (в соответствии с политикой безопасности, принятой в Вашей компании). Чтобы изменить ограничения на срок действия пароля, откройте Редактор групповых политик (Group Policy Editor) и выберите Конфигурация компьютера (Computer Configuration) - Конфигурация Windows (Windows Settings) - Параметры безопасности (Security Settings) - Политики учетных записей (Account Policies) - Политика паролей (Password Policy). Для внесения изменений дважды щелкните мышью на позиции "Макс. срок действия пароля" (Maximum password age), установите нужное значение в появившемся окне и нажмите "ОК". Изменения вступят в силу после применения групповой политики. | | |
| **Недостаток механизма безопасности:**  Использование ПО, не предназначенного непосредственно для работы АТМ | | |
| **Описание:**  Выявлен ряд эксплойтов, позволяющих использовать уязвимости прикладного ПО, которое установлено в Системе, но не предназначено для непосредственной работы банкомата, например:  • Выполнение произвольного кода в Adobe Flash Player (CVE-2007-3456);  • Выполнение произвольного кода в Adobe Flash Player (CVE-2012-1535);  • Использование после освобождения в Microsoft Internet Explorer ([CVE-2014-1776](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1776)).  Атака на прикладное ПО возможна в случае, когда злоумышленник имеет возможность запустить данное ПО, то есть имеет доступ к ОС банкомата в результате эксплуатации других уязвимостей. | | |
| **Рекомендации:**  Рекомендуется удалить из Системы все ПО, которое не предназначено для непосредственной работы банкомата. Если такое ПО невозможно удалить из Системы, необходимо использовать ПО контроля целостности, не внося непредназначенное для работы банкомата ПО в список доверенного. | | |

# Приложение А. Реестр уязвимостей

| **Уязвимость или недостаток механизма безопасности** | **Угроза** | **Уровень риска** | **Сложность** | **Описание** |
| --- | --- | --- | --- | --- |
| **Уязвимости** | | | | |
| Использование устаревших версий прикладного ПО и ОС | Получение полного контроля над ОС банкомата, вплоть до несанкционированной выдачи денежных средств | **Высокий** | **Средняя**  (для эксплуатации уязвимости необходим доступ к сети, к которой подключен банкомат, либо локальный доступ к ОС) | **Описание:**  В банкомате используется устаревшая версия ОС, для которой не осуществляется поддержка производителя. Также выявлено использование устаревших версий ПО. Злоумышленник может эксплуатировать уязвимости прикладного ПО и ОС, в том числе с применением общедоступных эксплойтов.  **Рекомендации:**  Необходимо удалить из Системы все ПО, которое не предназначено для работы банкомата. В случае невозможности удаления ПО (например, если прикладное ПО поставляется как неотъемлемый компонент ОС), следует использовать средства защиты, ограничивающие выполнение ПО (используемое на текущий момент McAfee Solidcore for APTRA либо аналог).  Обновить используемые ОС и прикладное ПО до актуальных версий. В случае, если своевременная установка актуальных обновлений ПО и ОС невозможна, принять компенсационные меры, такие как регистрация и мониторинг событий безопасности. |
| Отсутствие механизмов противодействия атакам ARP Cache Poisoning | Перехват сетевого трафика, отказ в обслуживании | **Средний** | **Средняя**  (для эксплуатации уязвимости необходимо подключение к сети банкомата) | **Описание:**  В сети не используются механизмы противодействия атакам ARP Cache Poisoning. Это может быть использовано для прослушивания трафика в сети Заказчика и проведения атак типа человек посередине. Нарушитель имеет возможность перехватывать конфиденциальную информацию, изменять данные в процессе передачи и блокировать сетевое взаимодействие.  **Рекомендации:**  Использовать статические ARP-записи для основных узлов сети.  Задействовать функции систем обнаружения атак, например, препроцессора arpspoof системы Snort (http://www.snort.org/), или утилиты, такие как arpwatch (http://xgu.ru/wiki/man:arpwatch).  Задействовать функции Dynamic ARP Inspection коммутаторов Cisco (http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/dynarp.pdf) или IP Source Guard. |
| Отсутствие MAC-значения в транзакционных запросах и ответах | Модификация трафика, несанкционированная выдача денежных средств | **Средний** | **Средняя**  (Для эксплуатации уязвимости необходимо подключение к сети банкомата) | **Описание:**  В используемом на тестовом стенде банкомате не включено добавление MAC-значения к транзакционным запросам и ответам, что позволяет модифицировать трафик без возможности обнаружения данной подмены банкоматом и процессинговым центром. Возможность модификации трафика позволяет увеличить количество выдаваемых банкнот и, таким образом, производить несанкционированную выдачу денежных средств.  **Рекомендации:**  Включить добавления MAC-значения ко всем запросам и ответам от сервера. |
| Отсутствие шифрования при взаимодействии между банкоматом и процессингом на прикладном уровне | Перехват сетевого трафика. Несанкционированная выдача денежных средств, раскрытие чувствительной информации, включая Track2 | **Средний** | **Средняя**  (Для эксплуатации уязвимости необходимо реализовать атаку «Человек посередине») | **Описание:**  Протокол NDC не предусматривает шифрования данных. При взаимодействии на прикладном уровне между банкоматом и процессинговым центром не обеспечивается шифрование, что позволяет злоумышленнику, осуществляющему атаку «человек посередине», перехватывать и модифицировать передающуюся информацию.  **Рекомендации:**  Обратиться к производителю программного обеспечения процессинга и банкомата для обеспечения шифрования на прикладном уровне либо обеспечить шифрование путем создания SSL-тоннеля. |
| Раскрытие чувствительной информации платежных карт | Раскрытие чувствительной информации (Track2) | **Средний** | **Средняя**  (Для эксплуатации уязвимости необходимо реализовать атаку «Человек посередине») | **Описание:**  Протокол NDC не предусматривает шифрования данных, а значение магнитной полосы Track2 передается в немаскированном виде. Таким образом, в результате прослушивания сетевого трафика нарушитель может перехватить немаскированное значение Track2 платежных карт.  **Рекомендации:**  Рекомендуется не передавать полное значение магнитной полосы Track2 в открытом виде, применив один из методов защиты: шифрование, маскирование, однонаправленные хэш-функции, токенизация. |
| Недостаточно надежная схема генерации симметричных ключей | Несанкционированная выдача денежных средств | **Средний** | **Высокая**  (Для эксплуатации уязвимости необходимо реализовать атаку «Человек посередине» на уровне USB, при этом требуется уровень квалификации, достаточный для анализа используемых алгоритмов обмена ключами и шифрования) | **Описание:**  Злоумышленник, зная значение параметра HDD\_ID, может по текущему времени процессора вычислить момент времени генерации стартового ключа и сгенерировать стартовый ключ самостоятельно. Чтобы расшифровать перехваченные данные злоумышленнику достаточно получить из стартового ключа последующие ключи с помощью описанного алгоритма.  Возможные атаки:   * Имея возможность выполнения кода в Системе, злоумышленник может прочитать файл data и получить из него два последних сессионных ключа и HDD\_ID. После этого можно атакующий может самостоятельно формировать команды на выдачу деньг для диспенсера, которые будут признаны валидными. * Зная HDD\_ID и перехватив одну валидную команду на выдачу денег злоумышленник может за разумное время (минуты, максимум - часы) найти текущее значение ключа, после чего использовать полученный ключ для расшифровки передаваемых данных или передачи собственных команд, которые будут признаны валидными. * Имея полный контроль над каналом между ОС и диспенсером в момент выработки стартового ключа, можно узнать его значение, выполнив атаку «человек посередине» при обмене ключами RSA.   **Рекомендации:**  Рекомендуется реализовать надежную схему генерации симметричных ключей путем:   * обфускации работы с сохраненными в файле data ключами; * изменения процедуры начальной инициализации PRNG в диспенсере, в частности не использовать time(NULL); * изменения процедуры генерации ключа в диспенсере (не использовать rand()); * использования сертификата для авторизации участников обмена при начальном обмене ключами через RSA для защиты от атак типа «человек посередине». |
| Отсутствует ограничение на минимальный срок действия пароля | Проведение атак на подбор пароля | **Средний** | **Высокая**  (Для эксплуатации уязвимости необходим доступ к ОС) | **Описание:**  Обнаружено, что минимальный срок действия пароля неограничен. Подобная политика может привести к повторному использованию паролей пользователями.  Minimum password age = 0.  <http://technet.microsoft.com/en-us/library/cc779758.aspx> <http://www.microsoft.com/technet/security/prodtech/windows2000/w2kccadm/acctpol/w2kadm07.mspx>.  **Рекомендации:**  Измените значение групповой политики на значение 1 или более дней (в соответствии с политикой безопасности, принятой в Вашей компании). Чтобы изменить ограничения на минимальный срок действия пароля, откройте Редактор групповых политик (Group Policy Editor) и выберите Конфигурация компьютера (Computer Configuration) - Конфигурация Windows (Windows Settings) - Параметры безопасности (Security Settings) - Политики учетных записей (Account Policies) - Политика паролей (Password Policy). Для внесения изменений дважды щелкните мышью на позиции "Мин. срок действия пароля" (Minimum password age), установите нужное значение в появившемся окне и нажмите "ОК". Изменения вступят в силу после применения групповой политики. |
| Отсутствует ограничение на минимальный срок действия пароля | Проведение атак на подбор пароля | **Средний** | **Высокая**  (Для эксплуатации уязвимости необходим доступ к ОС) | **Описание:**  Обнаружено, что максимальный срок действия пароля слишком велик или неограничен. Это может привести к успешным атакам подбора пароля.  Maximum password age = forever.  <http://technet.microsoft.com/en-us/library/cc736566.aspx> <http://www.microsoft.com/technet/security/prodtech/windows2000/w2kccadm/acctpol/w2kadm07.mspx>.  **Рекомендации:**  Измените значение групповой политики на значение 30-60 дней (в соответствии с политикой безопасности, принятой в Вашей компании). Чтобы изменить ограничения на срок действия пароля, откройте Редактор групповых политик (Group Policy Editor) и выберите Конфигурация компьютера (Computer Configuration) - Конфигурация Windows (Windows Settings) - Параметры безопасности (Security Settings) - Политики учетных записей (Account Policies) - Политика паролей (Password Policy). Для внесения изменений дважды щелкните мышью на позиции "Макс. срок действия пароля" (Maximum password age), установите нужное значение в появившемся окне и нажмите "ОК". Изменения вступят в силу после применения групповой политики. |
| Отсутствие аутентификации и шифрования данных при обмене информацией с кардридером | Раскрытие чувствительной информации платежных карт | **Низкий** | **Средняя** (Для эксплуатации уязвимости необходимо реализовать атаку «Человек посередине» между ОС и кардидером по USB) | **Описание:**  Используя отсутствие аутентификации при обмене трафиком с кардридером, нарушитель способен подключиться к USB-порту и перехватить содержимое магнитных дорожек платежных карт, передаваемое в открытом виде.  **Рекомендации:**  Рекомендуется не передавать полное значение магнитной полосы Track2 в открытом виде, применив один из методов защиты: шифрование, маскирование, однонаправленные хэш-функции, токенизация. |
| Недостаточная защита взаимодействия с периферийными устройствами | Несанкционированная выдача денежных средств, раскрытие чувствительной информации платежных карт. | **Низкий** | **Средняя** (Для эксплуатации уязвимости необходим доступ к ОС банкомата) | **Описание:**  В XFS не предусмотрено шифрования данных и механизма авторизации. Таким образом, любому приложению, работающему через XFS, доступно управление устройствами банкомата. Например, чтение информации с магнитной дорожки платежных карт (получение дорожки карты в открытом виде), а также выдача денежных средств.  **Рекомендации:**  Рекомендуется инициировать взаимодействие с производителем для изменения API и поддержки авторизации доступа к устройствам. Обеспечить эксклюзивное открытие логических устройств функцией WFSLock. |
| **Недостатки механизмов безопасности** | | | | |
| Недостаточно эффективная защита от выхода из киоска KeyBoardDisabler | Получение полного контроля над Системой, несанкционированная выдача денежных средств, раскрытие чувствительной информации. |  |  | **Описание:**  Злоумышленник может использовать активные «горячие клавиши» для выхода из режима киоска. Например, закрыть интерфейс ПО банкомата стандартным сочетанием клавиш (Alt+F4), а также закрыть само приложение KeyBoardDisabler нажатием любой клавиши, после чего станут доступны клавиши букв.  **Рекомендации:**  Отключить стандартные сочетания клавиш, показывать основное окно приложения APTRA поверх всех окон, отключить показ панели задач, изменить способ блокирования нажатий клавиш (убрать/спрятать приложение KeyBoardDisabler) |
| Недостаточная защита данных при их передаче между банкоматом и процессинговым центром | Раскрытие чувствительной информации. |  |  | **Описание:**  Используемые схемы подключения не обеспечивают достаточной защиты от перехвата и модификации передаваемой информации.  **Рекомендации:**  Необходимо реализовывать шифрование на уровне прикладных протоколов взаимодействия с процессинговым центром. Промежуточным решением может быть использование программного обеспечения STunnel для организации безопасных подключений, которые не могут быть отправлены в сеть по небезопасному каналу.  На уровне организации сетевого взаимодействия рекомендуется по возможности придерживаться варианта использования аппаратного VPN-клиента, размещаемого в пределах сервисной зоны банкомата. |
| Возможность загрузки сторонней ОС с внешних носителей | Получение полного контроля над системой, проведение атак, вплоть до несанкционированной выдачи банкнот |  |  | **Описание:**  Выявлено, что настройками BIOS разрешена загрузка сторонней ОС с внешнего USB-носителя. При этом нет необходимости авторизации в BIOS. Нарушитель может осуществить загрузку ОС с внешнего носителя и получить полный контроль над системой, проводить атаки с целью несанкционированной выдачи банкнот.  **Рекомендации:**  Запретить возможность загрузки ОС с внешних носителей в настройках BIOS. |
| Уязвимая реализация подключения к процессинговому центру | Подмена процессингового центра, проведение атак, в том числе несанкционированная выдача денежных средств |  |  | **Описание:**  В Системе реализовано прямое незащищенное подключение к процессинговому центру. Нарушитель может осуществить подмену процессингового центра и проводить атаки с целью несанкционированной выдачи банкнот.  **Рекомендации:**  Рекомендуется использовать для подключения к процессинговому центру аппаратный VPN-клиент, расположенный внутри сервисной зоны банкомата. |
| Использование ПО, не предназначенного непосредственно для работы АТМ | Проведение атак на ОС |  |  | **Описание:**  Выявлен ряд эксплойтов, позволяющих использовать уязвимости прикладного ПО, которое установлено в Системе, но не предназначено для непосредственной работы банкомата, например:  • Выполнение произвольного кода в Adobe Flash Player (CVE-2007-3456);  • Выполнение произвольного кода в Adobe Flash Player (CVE-2012-1535);  • Использование после освобождения в Microsoft Internet Explorer ([CVE-2014-1776](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1776)).  Атака на прикладное ПО возможна в случае, когда злоумышленник имеет возможность запустить данное ПО, то есть имеет доступ к ОС банкомата в результате эксплуатации других уязвимостей.  **Рекомендации:**  Рекомендуется удалить из Системы все ПО, которое не предназначено для непосредственной работы банкомата. Если такое ПО невозможно удалить из Системы, необходимо использовать ПО контроля целостности, не внося непредназначенное для работы банкомата ПО в список доверенного. |

# Приложение Б. Перечень установленного ПО

|  |  |
| --- | --- |
| Программное обеспечение | |
| .NET 2.x Runtime 02.02.0001 | PcQwertyKeyboard 01.00.00 |
| .NET Assemblies for Advance NDC | PcSound 04.00.00 |
| .NET Runtime 1.1.0000 | PcVideoCamera 01.03.01 |
| 3rd Party Runtime 02.01.01 | PresentationClient 2.9.1 |
| ActiveXFS Controls 02.12.00 | Problem Determination Collection 2.07.0251 |
| Adobe Flash Player 6.0.88.0 ActiveX | Realtek High Definition Audio Driver |
| Advance NDC 03.04.00 | Realtek AC'97 Audio 5.18 |
| Advance NDC Display Manager 03.00.03 | Resource Manager 02.01.01 |
| ANDCSP 03.04.00 | RS232ExteriorTouchScreen 02.03.00 |
| APTRA SST X.25 LAPB X.21 bis 02.02.01 | RS232PCDIPCardReader 02.02.00 |
| Bankom Video Exits 4.6 | RS232SwipeCardReader 03.00.00 |
| BPTRSP 91.03.0303 | Security 03.00.05 |
| Business Services Interfaces 02.03.01 | Self-Service Support Keyboards Configuration 04.00.00 |
| CCM PCCM 2.00.04 | Self-Service Support Runtime 03.00.02 |
| CCM VISA2 91.00.05.53 | Sentinel System Driver Installer 7.4.0 |
| Communications 92.05.01.53 | Serial Detector 02.00.00 |
| Data Manipulation 02.01.06 | SM Primitives 02.00.01 |
| DebugView 4.21 | SNMP Agent 3.04.01 |
| DevMan 01.00.00 | SNMP Master Agent 01.02.00 |
| ECB6Database 01.00.00 | Talladega Chipset 01.00.00 |
| EMV CAM2 Exits for APTRA Advance NDC 92.02.02.10 | Talladega Sound 1.0.0 |
| EMV\CAM2 Exits for Advance NDC 92.02.02.10 | TouchScreens 03.00.00 |
| Exception Handling 03.00.00 | USB Encrypting Pin Pad 01.00.00 |
| FeatureSupport 1.0.0.0 | USB Encrypting Pin Pad 2 1.0.0 |
| FLM\_2004 1.0.0.0 | USB Integrated Motorised Card Reader Writer 1.0.0 |
| FLM\_2008 1.0.0.0 | USB Loader Service 1.0.0 |
| FLM\_2012 1.0.0.0 | USB2DBarcodeReader 1.0.0 |
| FLM\_6618 1.0.0.0 | USB3MTch 01.00.00 |
| FLM\_6625 1.0.0.0 | USB80MM 1.0.0 |
| FLM\_6626 1.0.0.0 | USBAcousticWaveTouchScreen 1.0.0 |
| FLM\_6628 1.0.0.0 | UsbCameraSystem 1.0.0 |
| FLM\_6631 1.0.0.0 | USBContactlessCardReader 1.0.0 |
| FLM\_6632 1.0.0.0 | USBCurrencyDispenser 1.0.0 |
| FLM\_6634 1.0.0.0 | USBEnvelopeDepository 1.0.0 |
| FLM\_6636 1.0.0.0 | USBGDSTouchscreen 91.00.01.03 |
| FLM\_6638 1.0.0.0 | USBMiscellaneousInterface 1.0.0 |
| FLM\_6642 1.0.0.0 | UsbSmartCardReader 1.0.0 |
| FLM\_6654 1.0.0.0 | USBStmt 1.0.0 |
| FLM\_Media 1.0.0.0 | USBTouchScreen 01.00.00 |
| FSD-RUS APTRA Advance NDC Package 03.04.02 | USBUop 01.00.00 |
| FSD-RUS APTRA XFS 05.01.00 | Windows Internet Explorer 8 (20090308.140743) |
| HICS Interfaces 02.02.04 | Windows XP Pro Service Pack 3 |
| Inside Out Networks Watchport/V Drivers (Remove only) | WinRAR 5.20 (32-bit) 5.20.0 |
| Intel(R) Graphics Media Accelerator Driver | WMIDProv 1.00.0000 |
| Intel(R) Management Engine Interface | XFS CAM Service Provider 2.0.0.0 |
| MEEICnf 01.00.00 | XFS CDM Service Provider 3.0.0.8 |
| Microsoft .NET Framework 1.1 (1.1.4322) | XFS Contactless Card Reader Service Provider 1.0.0 |
| Microsoft .NET Framework 2.0 Service Pack 2 (2.2.30729) | XFS EDEP Service Provider 3.0.0.5 |
| Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 | XFS IDC Service Provider 3.0.0.5 |
| Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 | XFS Logical Name Resolver 1.0.0 |
| Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 | XFS Manager 3.0.0.0 |
| Mode Switch 03.01.00 | XFS PIN Service Provider 3.0.0.0 |
| MT 7.11 SR2 Software for Windows 2000 or XP | XFS PTR Service Provider 1.0.0.4 |
| NCR APTRA Dialogs 02.00.03 | XFS SIU Service Provider 3.0.0.3 |
| PC Communications Module Subsystem 92.00.00.55 | XFS TTU Service Provider 3.0.0.0 |
| PcAcousticWaveTouchScreen 03.01.00 | XFS VDM Service Provider 3.0.0.3 |
| PCISerial 01.00.02 | XFS UPTR Service Provider 1.0.0 |
| PcMonitor 1.0.0 |  |

1. В рамках работ по проверке корректности устранения уязвимостей специалисты Исполнителя выявили недостатки конфигурации BIOS, которые позволяют загрузку сторонней ОС с внешнего носителя (USB) без доступа к BIOS (см. Рисунок 4 и Рисунок 5). Необходимо запретить загрузку ОС с внешних носителей в настройках BIOS. [↑](#footnote-ref-2)
2. Уязвимость устранена путем удаления ПО Zytronic UPDD из состава ПО Системы. [↑](#footnote-ref-3)
3. Уязвимость устранена путем удаления ПО Zytronic UPDD из состава ПО Системы. [↑](#footnote-ref-4)
4. Уязвимость устранена путем удаления ПО Intellect из состава ПО Системы. [↑](#footnote-ref-5)
5. Уязвимость устранена путем удаления ПО McAfee Solidcore for APTRA из состава ПО Системы. [↑](#footnote-ref-6)
6. Уязвимость устранена путем удаления ПО McAfee Solidcore for APTRA из состава ПО Системы. [↑](#footnote-ref-7)