Отчет о результатах проверки корректности устранения уязвимостей стенда на базе банкомата NCR Personas 77  
АКБ "РосЕвроБанк" (ОАО)

Москва, 2015

Оглавление

[Оглавление 2](#_Toc426533544)

[Обозначения и сокращения 3](#_Toc426533545)

[1. Введение 4](#_Toc426533546)

[1.1. Общие сведения 4](#_Toc426533547)

[1.2. Цели проведения работ 4](#_Toc426533548)

[1.3. Описание проекта 4](#_Toc426533549)

[2. Методика проведения работ 5](#_Toc426533550)

[2.1. Условия и порядок проведения работ 5](#_Toc426533551)

[2.2. Модель нарушителя 5](#_Toc426533552)

[2.3. Оценка уровня критичности уязвимостей 6](#_Toc426533553)

[3. Описание объекта исследования 7](#_Toc426533554)

[4. Результаты работ 9](#_Toc426533555)

[5. Результаты проверки устранения уязвимостей 13](#_Toc426533556)

[6. Инструментальное сканирование Системы 16](#_Toc426533557)

[7. Результаты анализа защищенности 22](#_Toc426533558)

[7.1. Checker ATM Security Agent 22](#_Toc426533559)

[7.2. Аппаратный VPN-клиент 24](#_Toc426533560)

[7.3. SNMP 24](#_Toc426533561)

[Приложение А. Реестр уязвимостей 26](#_Toc426533562)

[Приложение Б. Перечень установленного ПО 34](#_Toc426533563)

# 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 «04» 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 «14» июля по «20» 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 Personas 77.

## 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 Системе 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 для проверки корректности устранения выявленных ранее уязвимостей в Системе использовалась комбинация инструментальных методов анализа и ручного исследования компонентов Системы экспертами. В рамках работ было проверенно наличие или отсутсвие в Системе всех уязвимостей, выяленных 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 набор устройств на базе банкомата NCR Personas 77 с ОС Windows XP Pro Service Pack 3 и набором ПО (см. Приложение Б), в том числе ПО Checker ATM Security Agent.

Исследуемая Система – тестовый стенд, соответствующий реально используемым банкоматам Заказчика по составу программного и программно-аппаратного беспечения. 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.



Рисунок . Объект исследования

Для проведения работ специалистами Заказчика 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.

Система состоит из системного блока банкомата и периферийных устройств, подключенных к нему через Sdc-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 2):

* **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 подключение к процессинговому центру с использованием аппаратного VPN-клиента. Аппаратный VPN-клиент расположен вне сервисной зоны банкомата и доступен любому внешнему нарушителю.

# Результаты работ

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

* **Выявлены возможности выхода из режима киоска, перехвата чувствительных данных (Track2) и реализации атак на ОС банкомата**, в следствие эксплуатации неустраненных Заказчиком уязвимостей. Большая часть уязвимостей (57,1% от общего числа) были устранены Заказчиком, что подтверждает проведенная проверка. При этом порядка одной трети (33,3% от общего числа) уязвимостей не были устранены, а для двух уязвимостей (9,5% от общего числа) не удалось реализовать проверку в рамках границ проведения работ. Невозможность проведения данных проверок обусловлена тем, что для проведения работ по проверке устранения уязвимостей Заказчиком была предоставлена система, отличная по составу программного и программно-аппаратного обеспечения от системы, расмотренной в рамках предыдущего проекта. Доля устраненных и не устраненных уязвимостей представлена на диаграмме ниже (см. Рисунок 3). Подробные результаты проверки устранения уязвимостей представлены в разделе 5 в Таблица 2.

Выявленные узявимости позволяют нарушителю перехватывать чувствительную инфомрацию в результате реализации атаки «Человек посередине». Также существует потенциальная возможность несанкционированной выдачи банкнот в результате реализации атак на ОС систему банкомата.

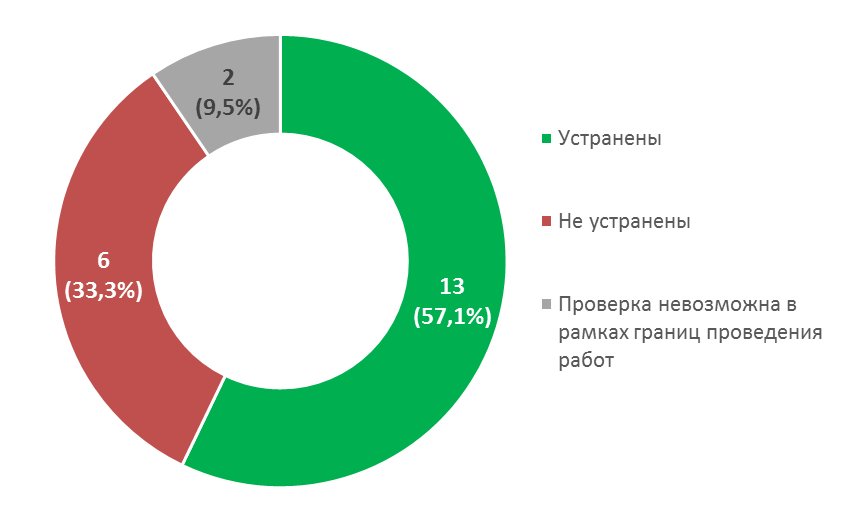


Рисунок . Доля устраненных и не устранённых уязвимостей

* **Выявлено 35 критических уязвимостей 7 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. 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.
* **Выявлена возможность загрузки ОС с внешних носителей в обход парольной защиты BIOS** в результате доступа к ПО Checker ATM Security Agent без аутентификации. Также нарушитель получает доступ к файловой системе банкомата. Парольная защита загрузчика Checker ATM Security Agent включена в настройках конфигурации серверной части данного ПО, но данная настройка оказалась не распространена на банкоматную часть ПО. Таким образом, нарушитель, обладающий доступом в сервисную зону банкомата может подключить клавиатуру и реализовать атаку. Учитывая, что в данной реализации Системы используется аппаратный VPN-клиент, расположенный вне сервисной зоны банкомата, любой внешний нарушитель может подключить свое программно-аппаратное обеспечение в разрыв между банкоматом и VPN-клиентом, и осуществлять атаки.

Также в рамках анализа защищенности было выявлено, что нарушитель может получать дополнительную инфомрацию о системе в результате использования стандартного значения SNMP Community String “public” с правами на чтение.

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** | **Средний** | В результате устранения уязвимостей специалисты Заказчика обеспечили добавление MAC-значений в транзакционные запросы и ответы, что позволяет обнаружить подмену данных между банкоматом и процессинговым центром и защитить Систему от атак с целью несанкционированной выдачи банкнот. При этом 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.  Подключение к процессинговому центру осуществляется посредством аппаратного VPN-клиента, расположенного вне сервисной зоны банкомата, что позволяет нарушиетелю 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. Существует возможность перехвата значений Track2.  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.  Выявлены недостатки межсетевого экранирования. Возможно получение расширенной инфомрации о системе в результате подключения к банкомату с использованием стандартного значения SNMP Community String “public” с правами на чтение. |
| **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 осуществить загрузку ОС с внешних носителей.  При этом 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 |
| 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[[1]](#footnote-2) |
| 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 | Уязвимость устранена |
| 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[[2]](#footnote-3) |
| Недостаточно надежная схема генерации симметричных ключей | Несанкционированная выдача денежных средств | Проверка невозможна в рамках границ проведения работ |
| Отсутствие аутентификации и шифрования данных при обмене информацией с кардридером | Раскрытие чувствительной информации платежных карт | Проверка невозможна в рамках границ проведения работ |
| Недостаточная защита взаимодействия с периферийными устройствами | Несанкционированная выдача денежных средств, раскрытие чувствительной информации платежных карт. | Уязвимость устранена |
| Выход за пределы киоска в ПО Intellect | Несанкционированный доступ к функциям ОС | Уязвимость устранена[[3]](#footnote-4) |
| 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[[4]](#footnote-5) |
| 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[[5]](#footnote-6) |
| 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. | Выявлена уязвимость |

# 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 42 уязвимости различной степени риска (см. Рисунок 4). Среди них 35 уязвимостей (83,3% от общего количества) являются критическими и 7 (16,7% от общего количества) – средней степени риска.

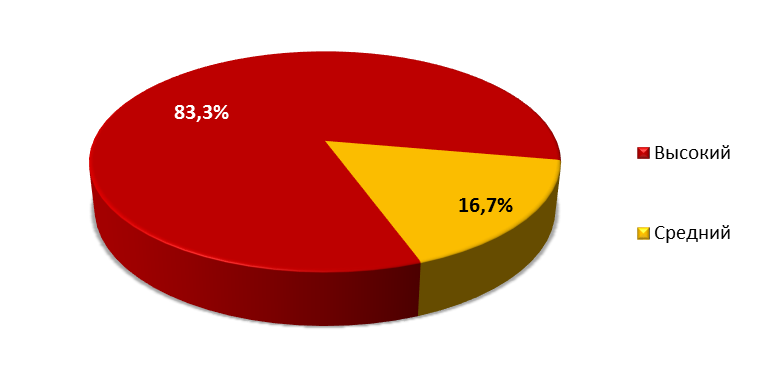


Рисунок . Доля выявленных уязвимостей различной степени риска

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 35, а уязвимостей средней степени риска со 118 до 7. 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.

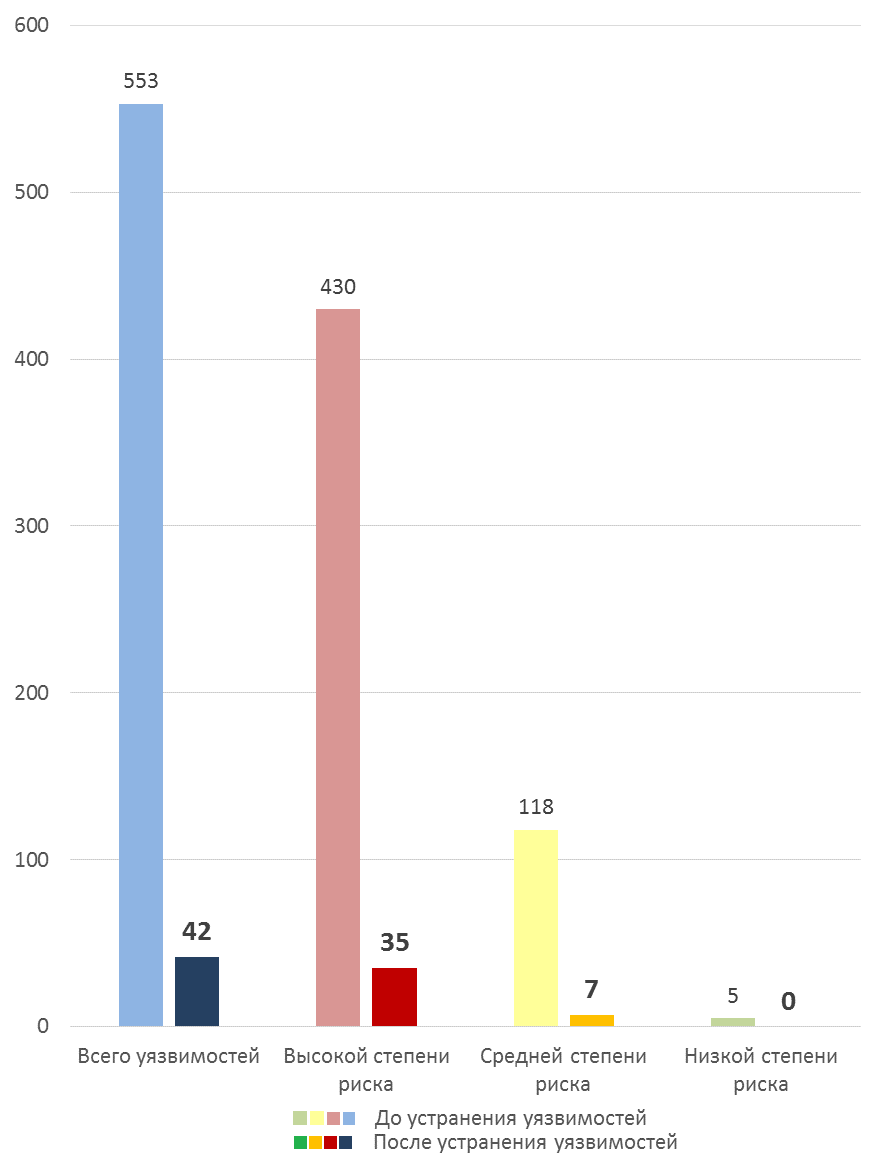


Рисунок . Количество выявленных уязвимостей до и после проведения работ по устранению уязвимостей (сравнительная диаграмма)

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-2010-0028 | 9.3 | Уязвимость при обработке целочисленных типов в MS Paint  <http://www.exploit-db.com/exploits/12518> |
| 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-2013-1347).

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 удалить его из списка доверенного ПО в системе Checker ATM Security Agent.

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 порядка 5% 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 проля равный 30 календарным дням. Обеспечить строгую парольную политику.

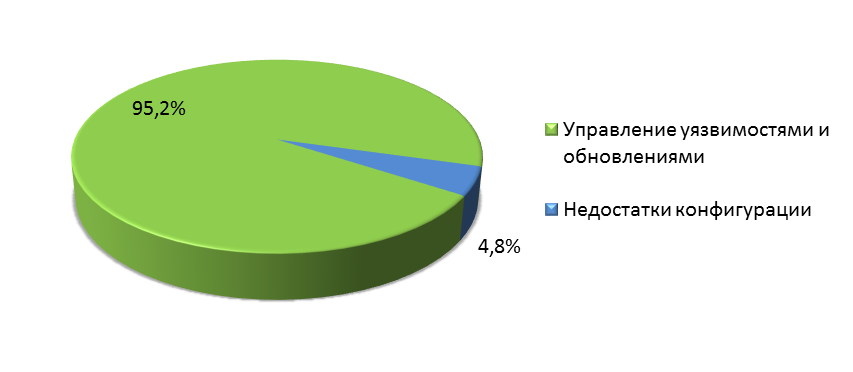


Рисунок . Доля выявленных уязвимости различных категорий

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. 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 (используемое на текущий момент Checker ATM Security Agent 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. | | |
| **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-2013-1347).  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 удалить его из списка доверенного ПО в системе Checker ATM Security Agent. | | |

# Результаты анализа защищенности

## Checker ATM Security Agent

Специалисты Исполнителя выявили, что на банкомате используется Checker ATM Security Agent (ПО для защиты банкомата). Данное ПО загружается до загрузки ОС банкомата. Политики безопасности настраиваются на стороне удаленного сервера ATMChecker и передаются на банкомат агенту. Анализ конфигурации серверной части ATMChecker показал, что доступ к загрузчику Checker ATM Security Agent на банкомате должен быть защищен паролем (см. Рисунок 7).

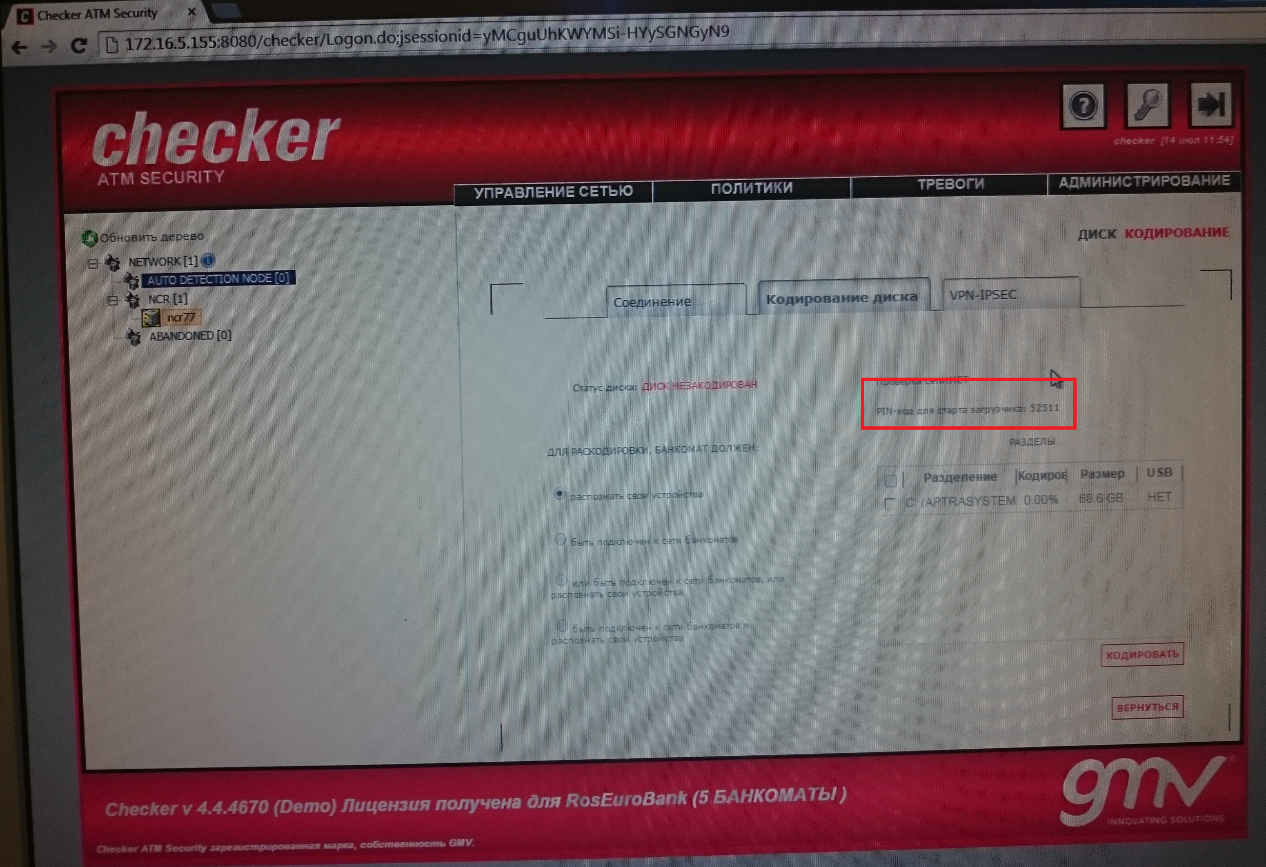


Рисунок . Серверная часть ATMChecker

В рамках работ специалисты Исполнителя выявили, что для доступа к загрузчику Checker ATM Security Agent на банкомате не требуется ввод пароля. Таким образом специалисты Исполнителя получили доступ к файловой системе банкомата (см. Рисунок 8 и Рисунок 9). Для реализации атаки необходим доступ к сервисной зоне банкомата и возможность подключения клавиатуры.

Используя данную уязвимость, атакующий может осуществить загрузку сторонней ОС с внешнего носителя (несмотря на парольную защиту BIOS и корректный порядок загрузки ОС).

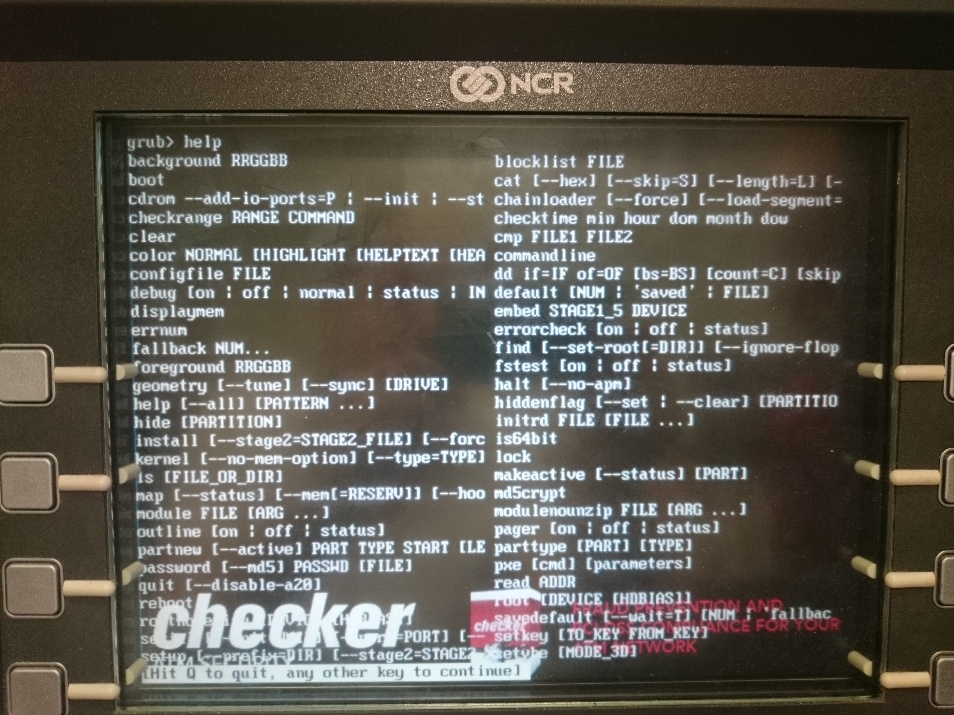


Рисунок . Список доступных команд

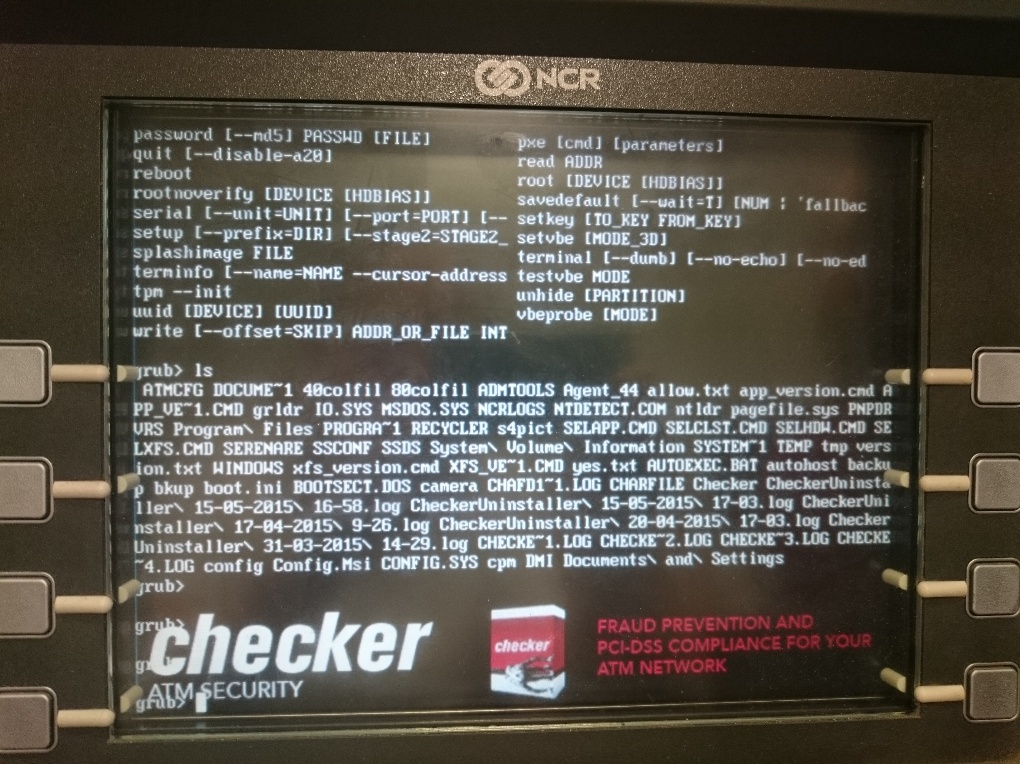


Рисунок . Доступ к файловой системе

|  |  |  |
| --- | --- | --- |
| **Уязвимость:**  Отсутствие аутентификации для доступа к ПО Checker ATM Security Agent | | |
| **Уровень риска: Высокий** | **CVSS: 7.2** (AV:L/AC:L/Au:N/C:С/I:С/A:С) | **Сложность:** Низкая |
| **Описание:**  На серверной части ПО для защиты банкомата ATMChecker включена парольная защита для доступа к загрузчику Checker ATM Security Agent. При этом выявлено, что доступ к ПО Checker ATM Security Agent на банкомате возможен без ввода пароля. Нарушитель получает доступ к файловой системе банкомата, а также получает возможность загружать стороннюю ОС с внешних носителей несмотря на парольную защиту BIOS. Для реализации атаки необходим доступ к сервисной зоне банкомата и возможность подключения клавиатуры. | | |
| **Рекомендации:**  Необходимо проверить корректность установки настроек защиты загрузчика Checker ATM Security Agent, которые должны управляться с серверной части данного ПО. Установить стойкий пароль для доступа к настройкам загрузчика Checker ATM Security Agent. Реализовать строгую парольную политику. | | |

## Аппаратный VPN-клиент

Также в рамках проведения работ было выявлено, что реализация VPN-подключения банкомата к процессинговому центру уязвима для атак со стороны внешнего нарушителя. В частности, аппаратный VPN-клиент расположен вне сервисной зоны банкомата. Такой способ подключения позволяет нарушителю подключить свое программно-аппаратное обеспечение в разрыв между банкоматом и VPN-клиентом и проводить атаки.

|  |
| --- |
| **Уязвимость:**  Уязвимая реализация VPN-подключения |
| **Описание:**  Реализация VPN-подключения банкомата к процессинговому центру уязвима для атак со стороны внешнего нарушителя. В частности, аппаратный VPN-клиент расположен вне сервисной зоны банкомата. Такой способ подключения позволяет нарушителю подключить свое программно-аппаратное обеспечение в разрыв между банкоматом и VPN-клиентом и проводить атаки. |
| **Рекомендации:**  Рекомендуется использовать для подключения к процессинговому центру аппаратный VPN-клиент, расположенный внутри сервисной зоны банкомата. |

## SNMP

Специалисты Исполнителя выявили недостатки межсетевого экранирования. В частности, возможно подключение к банкомату с использованием стандартного значения Community String “public” с привилегиями на чтение. Нарушитель может получить расширенную информацию о системе, которая затем может быть использована для реализации атак.

|  |  |  |
| --- | --- | --- |
| **Уязвимость:**  Использование словарных значений SNMP Community String | | |
| **Уровень риска: Средний** | **CVSS**: **5.0** (AV:N/AC:L/Au:N/C:P/I:N/A:N) | **Сложность:** Низкая |
| **Описание:**  Значение «public» (только чтение) для SNMP Community String позволяет получить расширенную информацию о системе, которая затем может быть использована злоумышленником для реализации других сценариев атаки. | | |
| **Рекомендации:**  Использовать значения SNMP Community String, отличные от значений по умолчанию. Отключить протокол SNMP, если он не используется. При использовании протокола рекомендуется переход к SNMPv3 для всех устройств, где на текущий момент используется более старая версия протокола. | | |
| **Недостаток механизма защиты:**  Недостаточное межсетевое экранирование | | |
| **Описание:**  Возможно подключение к банкомату по протоколу SNMP, что свидетельствует о недостаточном межсетевом экранировании либо о его отсутствии. | | |
| **Рекомендации:**  Настроить межсетевой экран, разрешив удаленное подключение только к необходимым для работы банкомата сервисам. Не оставлять открытыми для удаленного подключения порты, необходимость доступа к которым отсутствует. Разрешить удаленное подключение к открытым портам только с определенных адресов администраторов Системы. | | |

# 

# Приложение А. Реестр уязвимостей

| **Уязвимость или недостаток механизма безопасности** | **Угроза** | **Уровень риска** | **Сложность** | **Описание** |
| --- | --- | --- | --- | --- |
| **Уязвимости** | | | | |
| Отсутствие аутентификации для доступа к ПО Checker ATM Security Agent | Получение полного контроля над ОС банкомата, вплоть до несанкционированной выдачи денежных средств | **Высокий** | **Низкая** | **Описание:**  На серверной части ПО для защиты банкомата ATMChecker включена парольная защита для доступа к загрузчику Checker ATM Security Agent. При этом выявлено, что доступ к ПО Checker ATM Security Agent на банкомате возможен без ввода пароля. Нарушитель получает доступ к файловой системе банкомата, а также получает возможность загружать стороннюю ОС с внешних носителей несмотря на парольную защиту BIOS. Для реализации атаки необходим доступ к сервисной зоне банкомата и возможность подключения клавиатуры.  **Рекомендации:**  Необходимо проверить корректность установки настроек защиты загрузчика Checker ATM Security Agent, которые должны управляться с серверной части данного ПО. Установить стойкий пароль для доступа к настройкам загрузчика Checker ATM Security Agent. Реализовать строгую парольную политику. |
| 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 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. |
| 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. |
| **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. |
| 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-2013-1347).  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 удалить его из списка доверенного ПО в системе Checker ATM Security Agent. |
| Уязвимая реализация VPN-подключения | Подмена процессингового центра, проведение атак, в том числе несанкционированная выдача денежных средств |  |  | **Описание:**  Реализация VPN-подключения банкомата к процессинговому центру уязвима для атак со стороны внешнего нарушителя. В частности, аппаратный VPN-клиент расположен вне сервисной зоны банкомата. Такой способ подключения позволяет нарушителю подключить свое программно-аппаратное обеспечение в разрыв между банкоматом и VPN-клиентом и проводить атаки.  **Рекомендации:**  Рекомендуется использовать для подключения к процессинговому центру аппаратный VPN-клиент, расположенный внутри сервисной зоны банкомата. |
| Недостаточное межсетевое экранирование | Проведение атак на Систему |  |  | **Описание:**  Возможно подключение к банкомату по протоколу SNMP, что свидетельствует о недостаточном межсетевом экранировании либо о его отсутствии.  **Рекомендации:**  Настроить межсетевой экран, разрешив удаленное подключение только к необходимым для работы банкомата сервисам. Не оставлять открытыми для удаленного подключения порты, необходимость доступа к которым отсутствует. Разрешить удаленное подключение к открытым портам только с определенных адресов администраторов Системы. |

# Приложение Б. Перечень установленного ПО

|  |  |
| --- | --- |
| Программное обеспечение | |
| .NET 2.x Runtime 02.00.01 | Realtek AC'97 Audio 5.18 |
| .NET Assemblies for Advance NDC | Resource Manager 02.01.01 |
| .NET Runtime 1.1.0000 | RS232BarcodeReader 02.00.02 |
| 3rd Party Runtime 02.01.01 | RS232ContactlessCardReader 1.0.0 |
| ActiveXFS Controls 02.12.00 | RS232DashCardReader 02.00.02 |
| Adobe Flash Player 6.0.88.0 ActiveX | RS232ExteriorTouchScreen 02.03.00 |
| Advance NDC 03.04.00 | RS232IMCRW 92.00.06.03 |
| Advance NDC Display Manager 03.00.03 | RS232PCDIPCardReader 02.02.00 |
| ANDCSP 03.04.00 | RS232SwipeCardReader 03.00.00 |
| APTRA SST X.25 LAPB X.21 bis 02.02.01 | Sdc Primary 03.00.00 |
| Bankom Video Exits 4.6 | SdcBape 05.00.01 |
| BPTRSP 91.03.0303 | SdcCurrencyDispenser 93.04.00.02 |
| Business Services Interfaces 02.03.01 | SdcDipCardReader 03.00.00 |
| CCM PCCM 2.00.04 | SdcEDep 03.00.07 |
| CCM VISA2 91.00.05.53 | SdcEkc 05.00.01 |
| Checker ATM Security Agent | SdcEop 03.00.00 |
| Communications 92.05.01.53 | SdcInfraRedTouchScreen 03.00.00 |
| Data Manipulation 02.01.06 | SdcMiscellaneousInterface 03.00.00 |
| DebugView 4.21 | SdcMotorisedCardReaderWriter 03.00.02 |
| DevMan 01.00.00 | SdcpStatementPrinter 02.00.02 |
| ECB6Database 01.00.00 | SdcRs232 03.00.00 |
| EMV CAM2 Exits for APTRA Advance NDC 92.02.02.10 | SdcStatementPrinter 03.00.02 |
| EMV\CAM2 Exits for Advance NDC 92.02.02.10 | Security 03.00.05 |
| Exception Handling 03.00.00 | Self-Service Support Keyboards Configuration 04.00.00 |
| FeatureSupport 1.0.0.0 | Self-Service Support Runtime 03.00.02 |
| FLM\_6674 1.0.0.0 | Sentinel System Driver Installer 7.4.0 |
| FLM\_6676 1.0.0.0 | Serial Detector 02.00.00 |
| FLM\_Media 1.0.0.0 | SM Primitives 02.00.01 |
| FSD-RUS APTRA Advance NDC Package 03.04.02 | SNMP Agent 3.04.01 |
| FSD-RUS APTRA XFS 05.01.00 | SNMP Master Agent 01.02.00 |
| HICS Interfaces 02.02.04 | TouchScreens 03.00.00 |
| Intel(R) Extreme Graphics Driver | USB Loader Service 1.0.0 |
| Intel(R) PRO Network Connections Drivers | USB2DBarcodeReader 1.0.0 |
| Keyboard/Mouse SSPB Kernel Subsystem 1.00.0000 | USB3MTch 01.00.00 |
| MEEICnf 01.00.00 | USBAcousticWaveTouchScreen 1.0.0 |
| Microsoft .NET Framework 1.1 (1.1.4322) | USBEnvelopeDepository 1.0.0 |
| Microsoft .NET Framework 2.0 (2.0.50727) | USBGDSTouchscreen 91.00.01.03 |
| Microsoft Kernel-Mode Driver Framework Feature Pack 1.9 | USBTouchScreen 01.00.00 |
| Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 | USBUop 01.00.00 |
| Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 | Windows Internet Explorer 8 (20090308.140743) |
| Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 | Windows XP Pro Service Pack 3 |
| Mode Switch 03.01.00 | WinRAR 5.20 (32-bit) 5.20.0 |
| NCR APTRA Dialogs 02.00.03 | WMIDProv 1.00.0000 |
| PC Communications Module Subsystem 92.00.00.55 | XFS CAM Service Provider 2.0.0.0 |
| Pc40ColumnThermalPrinters 03.00.05 | XFS CDM Service Provider 3.0.0.8 |
| Pc60mmThermalPrinter 02.00.02 | XFS Contactless Card Reader Service Provider 1.0.0 |
| PcAcousticWaveTouchScreen 03.01.00 | XFS EDEP Service Provider 3.0.0.5 |
| PCISerial 01.00.02 | XFS IDC Service Provider 3.0.0.5 |
| PcMiscellaneousInterface 03.00.00 | XFS Logical Name Resolver 1.0.0 |
| PcMonitor 1.0.0 | XFS Manager 3.0.0.0 |
| PcQwertyKeyboard 01.00.00 | XFS NDEP Service Provider 3.0.0.5 |
| PcSound 04.00.00 | XFS PIN Service Provider 3.0.0.0 |
| PcVideoCamera 01.03.01 | XFS PTR Service Provider 1.0.0.4 |
| PIVAT Chipset 01.00.00 | XFS SIU Service Provider 3.0.0.3 |
| PIVAT Sound 01.00.02 | XFS TTU Service Provider 3.0.0.0 |
| PresentationClient 2.9.1 | XFS VDM Service Provider 3.0.0.3 |
| Problem Determination Collection 2.08.0051 |  |

1. Уязвимость устранена путем удаления ПО Zytronic UPDD из состава ПО Системы. [↑](#footnote-ref-2)
2. Уязвимость устранена путем удаления ПО Zytronic UPDD из состава ПО Системы. [↑](#footnote-ref-3)
3. Уязвимость устранена путем удаления ПО Intellect из состава ПО Системы. [↑](#footnote-ref-4)
4. Уязвимость устранена путем удаления ПО McAfee Solidcore for APTRA из состава ПО Системы. [↑](#footnote-ref-5)
5. Уязвимость устранена путем удаления ПО McAfee Solidcore for APTRA из состава ПО Системы. [↑](#footnote-ref-6)