|  |  |  |  |
| --- | --- | --- | --- |
| № | Уязвимость | Угроза | Сценарий атаки |
| 1 | Уязвимость точки доступа Wi-Fi, связанная с отключенными параметрами скрытности точки доступа, позволяющая злоумышленнику подделать ее с такими же характеристиками | Угроза нескрытных точек доступа заключается в возможности злоумышленника получения информации о характеристиках легитимной точки доступа и создания поддельной с аналогичными характеристиками, что может привести к краже парольной информации для аутентификации в сети WLAN или к нарушению работы системы. | С помощью функции «airodump-ng» утилиты «Aircrack-ng» и переведенной сетевой карты в режим «Монитор» злоумышленник может узнать характеристики точки доступа Wi-Fi такие как: ее SSID, MAC-адрес, рабочий канал, режим шифрования и другие.  Далее создает поддельную точку доступа с аналогичными характеристиками и может выполнить следующие атаки: |
|  |  |  | «Cafe-Latte» - когда злоумышленник может узнать WEP – ключ сети (функция «aireplay-ng»),  «Becon» - когда создаются поддельные точки легитимной сети Wi-Fi и клиентское устройство не может подключиться и остается в статусе «ожидание подключения»,  FDI – навязывания ложных данных (подмена), MiTM, нарушение целостности и доступности данных и др. |
| 2 | Уязвимость микропрограммного обеспечения модуля ESP8266, позволяющая вызвать переполнение буфера и отказ в обслуживании модуля | Угроза несанкционированного управления буфером заключается в возможности осуществления нарушителем деструктивного программного воздействия на систему. | При подключении к точке доступа последняя отправляет ESP8266 пакет «AKM suite count», который содержит количество методов аутентификации, доступных для соединения.  Поскольку ESP8266 не выполняет проверку границ для этого значения, поддельная точка доступа может отправить слишком большое число, что приведёт к переполнению буфера и сбою ESP. Таким образом, злоумышленник может отправить ESP8266 фальшивый маячковый или ответный фрейм в |
|  |  |  | зависимости от режима работы Wi-Fi точки, тем самым вызвать отказ в обслуживании аппаратного обеспечение модуля. |
| 3 | Уязвимость идентификации устройств Wi-Fi-модулей ESP8266, позволяющая злоумышленнику внедрить несанкционированное устройство в сеть WLAN и влиять на работу системы. | Угроза обработки данных от неавторизированных устройств заключается в отсутствии проверки идентификаторов устройств и соответствующих подтверждающих факторов переданных ими данных. | Из-за отсутствия идентификации устройств, программного ограничения на количество подключенных устройств или многофакторной проверки целостности данных злоумышленник может внедрить несанкционированное устройство в сеть Wi-Fi (для этого необходимо получить WEP-ключ сети) и выполнять атаки FDI, подмены данных системы, тем самым нарушая ее работу. |
| 4 | Уязвимость программного обеспечения системы, связанной с однофакторной проверкой целостности информации, позволяющая злоумышленнику подделывать передаваемые данные. |
| 5 | Уязвимость реализации протокола TCP, позволяющая сбросить TCP – соединение. | Угроза несанкционированного отключения устройств системы заключается в возможности злоумышленника, подделав IP-устройства, отправить от его имени TCP-пакет с флагом «RST» - немедленному прекращению соединения. | Атака «TCP - RST» аналогична атаке деаутентификации клиентов от точки доступа, но только разрывает TCP – соединение с сервером. Так как в модели для передачи данных по Wi-Fi, на точке доступа развернут TCP-сервер, к которому подключается контроллер датчиков. Проведя атаку «TCP - RST», например, инструментом «Netwox 40», злоумышленник прервет сеанс передачи данных и нарушит работу системы, однако разрыва Wi-Fi соединения не произойдет. Причину нарушения работы можно будет выявить только проанализировав сетевой трафик системы. |
| 6 | Уязвимость микропрограммного обеспечения модуля радио NRF24L01, связанная с незашифрованной передачей полезных данных, позволяющая злоумышленнику получить конфиденциальную информацию | Угроза перехвата данных, заключается в отсутствии криптографических алгоритмов защиты информации и в возможности злоумышленника ознакомления с передаваемыми полезными данными, а вследствие их подделывания и внедрения в канал связи. | Злоумышленнику достаточно узнать рабочий канал работы радиомодуля, например с использованием анализатора спектра частоты 2.4 ГГц или широкополосного программно-определяемого радио приемо-передатчика «HackRF», который способен на заданной частоте принимать и передавать данные, а также создавать на ней помехи. |
| 7 | Уязвимость микропрограммного обеспечения контроллеров, позволяющая вызвать переполнение буфера и отказ в обслуживании контроллера | Угроза несанкционированного управления буфером заключается в возможности осуществления нарушителем деструктивного программного воздействия на систему. | Атаку на переполнение буфера без физического доступа к контроллеру можно выполнить, используя модуль связи, к которому он подключен. Так, в модели используется радиомодуль NRF24L01, прием данных с которого осуществлен с помощью статического массива заданной длины. Таким образом, злоумышленник может собрать свое устройство с таким же модулем, запрограммировать его на передачу данных на одном из каналов (всего их 127) или на всех поочередно и ждать, когда атакованный контроллер выйдет из строя из-за переполнения буфера. |