DOI: 10.58168/MoInSyTe2024_365-370
УДК 004.9

СОВРЕМЕННЫЕ УЯЗВИМОСТИ БЕСПРОВОДНЫХ СЕТЕЙ И МАРШРУТИЗАТОРОВ

Д.Г. Пахомов[1], В.И. Анциферова[1], Ю.А. Чевычелов[1]

[1]ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. В работе рассматриваются принципы работы и основы Wi-Fi сетей, их безопасность и средства защиты.

Ключевые слова: Wi-Fi, беспроводные сети, безопасность, протокол безопасности, хакерские атаки.

MODERN VULNERABILITIES OF WIRELESS NETWORKS AND ROUTERS

D.G. Pakhomov[1], V.I. Antsiferova[1], Yu.A. Chevychelov[1]

[1]Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. The paper discusses the principles of operation and fundamentals of Wi-Fi networks, their security and means of protection.

Keywords: Wi-Fi, wireless networks, security, security protocol, hacker attacks.

В настоящей эпохе цифровизации и постоянного прогресса технологий Wi-Fi сети стали неотъемлемой частью нашей повседневной жизни. Более того, они являются основой для подключения множества устройств, таких как смартфоны, планшеты, ноутбуки и даже умные домашние устройства. Однако, несмотря на все их преимущества, Wi-Fi сети также оказались подвержены различным уязвимостям в последние годы.

В данной статье будет рассмотрены некоторые из наиболее актуальных уязвимостей Wi-Fi сетей, маршрутизаторов и предоставлены рекомендации по их преодолению.

Недостаток в структуре стандарта IEEE 802.11. Данный недостаток вынуждает точки доступа передавать сетевые кадры в формате простого текста. Кадры или фреймы Wi-Fi (WiFi frame) представляют собой контейнеры данных, состоящие из заголовка, полезной нагрузки и трейлера. Они содержат такую информацию, как MAC-адрес источника и пункта назначения, а также данные для контроля и управления.Кадры упорядочиваются и имеют очередность, передаваясь контролируемым образом, чтобы избегать коллизий и максимизировать производительность обмена данными путем мониторинга состояний busy/idle для точек приема. Исследователи обнаружили, что упорядоченные/буферизованные кадры недостаточно защищены от злоумышленников, которые в итоге получают возможность манипулировать передачей данных, осуществлять спуфинг клиента, перенаправление и перехват кадров. «Описанная атака имеет масштабное влияние, так как затрагивает различные устройства и операционные системы (Linux, FreeBSD, iOS и Android), а также может быть использована для перехвата TCP-соединений, клиентского и сетевого трафика», – пишут специалисты. Проблема заключается в том, что стандарт IEEE 802.11 имеет энергосберегающие механизмы, которые позволяют устройствам экономить энергию за счет буферизации или постановки в очередь кадров, предназначенных для «спящих» устройств.

То есть, когда клиентская станция (принимающее устройство) переходит в спящий режим, она отправляет точке доступа кадр со специальным заголовком, содержащим «энергосберегающий» бит, после чего все кадры, предназначенные для этой станции, ставятся в очередь. Как только клиентская станция просыпается, точка доступа извлекает буферизованные кадры из очереди, шифрует и передает адресату.Однако стандарт не содержит явных указаний по управлению безопасностью для таких кадров в очереди, а также не устанавливает ограничений (например, не определяет, как долго кадры могут оставаться в таком состоянии).Эксперты объясняют, что злоумышленник может подделать MAC-адрес устройства в сети и передать «энергосберегающие» кадры точке доступа, вынудив ее поставить в очередь кадры, предназначенные для жертвы. После этого атакующий передает точке доступа кадр пробуждения и получает кадры из очереди.

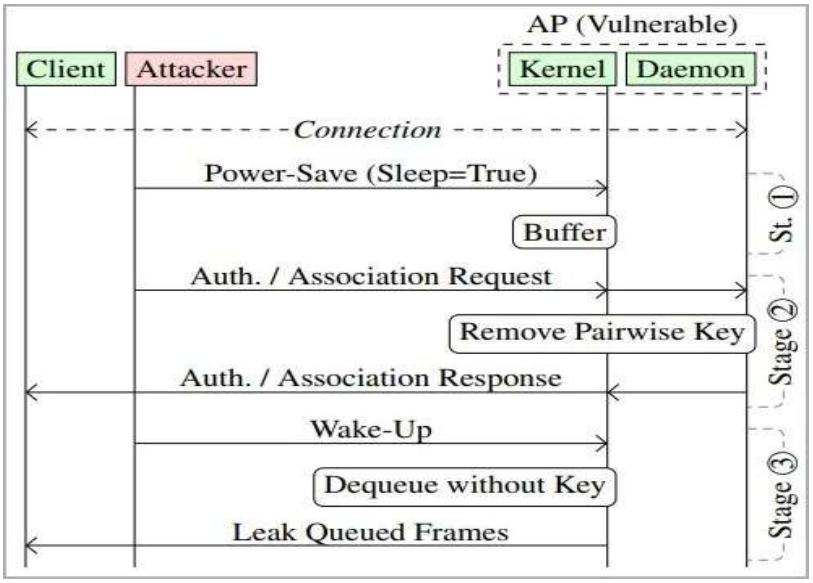

Рисунок 1 – Схема атаки

Доклад специалистов гласит, что передаваемые кадры обычно шифруются с помощью группового ключа шифрования, общего для всех устройств в сети Wi-Fi, или парного ключа шифрования, который уникален для каждого устройства и используется для шифрования кадров, которыми обмениваются конкретные устройства. Но злоумышленник может передать точке доступа кадры аутентификации и ассоциации, тем самым заставив ее передавать кадры в виде простого текста или шифровать их ключом, предоставленным самим атакующим.Перед такими атаками уязвимы самые разные модели сетевых устройств, производства Lancom, Aruba, Cisco, Asus и D-Link. Список протестированных специалистами девайсов приведен ниже.

Hardware	Software	SCO	FR
LANCOM LN-1700	10.42.0255	●	●
Aruba AP-305/7008	ArubaOS 8.4.0.0	●	●
Cisco Catalyst 9130	IOS XE 17.2.1.11	●	○
Hostapd on Linux	Version 2.10	●	●
Asus RT-AC51U	3.0.0.4.380_8591	●	○
D-Link DIR-853	ET853pnp-1.05-b55 [1]	●	—
D-Link DIR-853	OpenWRT 22.03	●	●
Cisco WAG320N	V1.00.08	●	—
Asus RT-N10	Tomato 1.28	●	—

Рисунок 2 – Уязвимый софт

Кроме того, исследователи предупреждают, что подобные атаки могут использоваться для внедрения вредоносного содержимого (например, JavaScript) в

TCP-пакеты. «Злоумышленник может использовать собственный сервер, подключенный к интернету, для инъекции данных в TCP-соединение путем инъекции off-path TCP-пакетов с поддельным IP-адресом отправителя. Это может быть использовано, например, для отправки вредоносного JavaScript-кода жертве в HTTP-соединениях с целью использования уязвимостей в браузере», — сообщается в отчете. Разработчики признают, что описанные атаки могут представлять угрозу для таких продуктов, как Cisco Wireless Access Point и Cisco Meraki с беспроводными возможностями. При этом, в компании отмечают, что полученные злоумышленником кадры вряд ли поставят под угрозу общую безопасность хорошо защищенной сети.

Блок уязвимостей маршрутизаторов, выявленных за март текущего 2024 года.

- Уязвимость интерфейса apply.cgi микропрограммного обеспечения маршрутизатора TRENDnet TEW-827DRU связана с непринятием мер по нейтрализации специальных элементов, используемых в команде ОС. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии до уровня root-пользователя путём изменения параметров почтового запроса usapps.config.smb_admin_name.

- Уязвимость функции formQuickIndex файла /goform/QuickIndex микропрограммного обеспечения маршрутизатора Tenda AC18 связана с возможностью чтения данных за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии путём записи специально сформированных данных в аргумент PPPOEPassword.

- Уязвимость службы HNAP микропрограммного обеспечения маршрутизаторов D-Link DIR-822 связана с возможностью переполнения буфера на основе стека. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код.

- Уязвимость функции fromSetlpMacBind() микропрограммного обеспечения маршрутизатора Tenda AC9 связана с чтением данных за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании.

- Уязвимость функции setDiagnosisCfg файла /cgi-bin/cstecgi.cgikомопнентashttpd микропрограммного обеспечения маршрутизатора Totolink X6000R су-

ществует из-за непринятия мер по нейтрализации специальных элементов, используемых в команде операционной системы. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код.

- Уязвимость функции fromSysToolRestoreSet() (/goform/SysToolRestoreSet) микропрограммного обеспечения маршрутизатора Tenda AC18 связана с недостаточной проверкой подлинности выполняемых запросов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, осуществить CSRF-атаку.

- Уязвимость микропрограммного обеспечения Wi Fi роутеров TP-Link Archer AX50 (AX3000) связана с непринятием мер по защите структуры веб-страницы. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный JavaScript-код при загрузке созданного правила перенаправления портов.

Меры по устранению/недопущению уязвимостей:

- использование систем обнаружения и предотвращения вторжений для отслеживания индикаторов компрометации;

- ограничение доступа из общедоступных сетей (Интернет);

- использование средств межсетевого экранирования уровня веб-приложений для ограничения возможности удалённого доступа;

- использование виртуальных частных сетей для организации удаленного доступа (VPN);

- отключение функционала удалённого администрирования;

- отключение/удаление неиспользуемых учётных записей пользователей;

- использование средств межсетевого экранирования и средств обнаружения и предотвращения вторжений (IDS/IPS) для отслеживания подключений к устройству.

Список литературы

1. Модификация метода поиска информации в сети интернет на основе использования методов индуктивного рассуждения / В. В. Лавлинский, А. Л. Савченко, И. А. Земцов, О. Г. Иванова // Моделирование систем и процессов. – 2019. – Т. 12, № 1. – С. 61-67.

2. Широкополосные беспроводные сети передачи информации / В. М. Вишневский [и др.]. - Москва: Техносфера, 2005. - 595 с.

3. Гордейчик С.В. Безопасность беспроводных сетей / С. В. Гордейчик, В. В. Дубровин. - Москва : Горячая линия - Телеком, 2008. - 288 с.

4. Технологии современных беспроводных сетей Wi-Fi. – Режим доступа: https://okwifi.com/soveti/standarty-wifi.html. – Заглавие с экрана.

5. Взлом беспроводной сети: способы и программы. – Режим доступа: https://tproger.ru/articles/vzlom-wi-fisposoby-i-programmy/. – Заглавие с экрана.

6. Wi-Fi сети: проникновение и защита. – Режим доступа: https://habr.com/ru/post/224955/. – Заглавие с экрана.

7. Полуэктов А. В., Макаренко Ф. В., Ягодкин А. С. Использование сторонних библиотек при написании программ для обработки статистических данных // Моделирование систем и процессов. – 2022. – Т. 15, № 2. – С. 33-41.

References

1. Modification of the method of searching for information on the Internet based on the use of inductive reasoning methods / V. V. Lavlinsky, A. L. Savchenko, I. A. Zemtsov, O. G. Ivanova // Modeling of systems and processes. – 2019. – vol. 12, No. 1. – pp. 61-67.

2. Broadband wireless information transmission networks / V. M. Vishnevsky [et al.]. - Moscow: Technosphere, 2005. - 595 p.

3. Gordeychik S. V. Security of wireless networks / S. V. Gordeychik, V. V. Dubrovin. - Moscow: Hotline - Telecom, 2008. - 288 p.

4. Technologies of modern wireless Wi-Fi networks. – URL: https://okwifi.com/soveti/standarty-wifi.html. – Title from the screen.

5. Hacking a wireless network: methods and programs. – URL : https://tproger.ru/articles/vzlom-wi-fisposoby-i-programmy /. – Title from the screen.

6. Wi-Fi networks: penetration and protection. – URL: https://habr.com/ru/post/224955 /. – Title from the screen.

7. Poluektov A. V., Makarenko F. V., Yagodkin A. S. The use of third-party libraries when writing programs for processing statistical data // Modeling of systems and processes. – 2022. – Vol. 15, No. 2. – pp. 33-41.