УДК 528.71
DOI 10.33764/2618-981X-2024-6-70-74

А. С. Зонов[1], А. В. Шабурова[1]*

Анализ уязвимостей сетевых устройств

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: alex301919@yandex.ru

Аннотация. Маршрутизаторы служат основой для координации трафика в любой сети, будь то масштабная корпоративная структура или домашняя среда. В организациях часто используется множество таких устройств, что усложняет контроль за их обновлениями и общим состоянием безопасности. Именно этими пробелами в защите и пользуются хакеры, а также производители с сомнительной репутацией. Для минимизации рисков, связанных с цифровыми угрозами, критически важно активно заниматься поддержанием информационной безопасности, проведением аудита и управленем сетевых устройств, чтобы предотвратить атаки еще на раннем этапе. У каждого такого устройства есть прошивка, которую специалисты могут проверить и обнаружить в ней как уязвимости, так и спланированно заложенные программные закладки, например, бекдоры, шеллы или же ботнеты. Для упрощения и ускорения этой работы можно использовать сканер прошивок.

Ключевые слова: PON, безопасность сети, аудит, маршрутизатор

A. S. Zonov[1], A. V. Shaburova[1]*

Analysis of network device vulnerabilities

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: alex301919@yandex.ru

Abstract. Routers constitute the fundamental infrastructure for traffic coordination within any network, be it an expansive corporate entity or a residential setting. A plethora of such devices is often employed within organizations, complicating the oversight of their firmware updates and the holistic state of security. It is these very lapses in defense mechanisms that are exploited by malicious actors, as well as manufacturers with questionable credentials. To mitigate risks associated with digital threats, it is imperative to proactively maintain information security, commencing with the auditing and management of the diversity of network devices, thus precluding the onset of adversarial attacks during the incipient stages.Each device is equipped with firmware that specialists are capable of scrutinizing for potential vulnerabilities and intentionally embedded software subversions, such as backdoors, shells, or botnets. To streamline and expedite this process, the deployment of a firmware scanner is advisable.

Keywords: PON, network security, router

Введение

В современном цифровом мире сетевые устройства стали неотъемлемой частью инфраструктуры любого предприятия и домашнего хозяйства. Одним из перспективных и широко распространённых видов оборудования для организа-

ции доступа в интернет являются PON (Passive Optical Network) [1] роутеры, используемые в оптоволоконных сетях для предоставления высокоскоростного доступа [2]. Они заменяют традиционные медные линии на оптоволокно, что позволяет достигать больших скоростей передачи данных [3]. Однако, как и любое другое сетевое оборудование, PON-роутеры подвержены уязвимостям, которые могут быть использованы злоумышленниками для атаки [4]. Поэтому анализ уязвимостей этих устройств становится критически важным для обеспечения безопасности сетевых систем и сохранности передаваемой информации [5].

Методика исследования

Команда OWASP, занимающаяся проблемами безопасности в области вебприложений [6]. Также обращает внимание на безопасность устройств, подключенных к Интернету. Хотя организация не фокусируется непосредственно на PON-роутерах, общие принципы безопасности, пропагандируемые OWASP, применимы и к этому типу устройств. К ним относятся: обеспечение своевременного обновления прошивок, использование сложных паролей и шифрование трафика, принцип наименьших привилегий для пользовательских учетных записей и применение межсетевых экранов для контроля трафика [7].

Анализ уязвимостей сетевых устройств

Проведение анализа уязвимостей PON-роутеров начинается с понимания их специфики. PON-роутеры часто имеют встроенное программное обеспечение от производителя, которое может содержать предустановленные настройки, уязвимые к целому ряду атак [8]. Исследования и отчеты по безопасности, например отчеты CERT (Computer Emergency Response Team), включают описание потенциальных недостатков и рекомендации по их устранению [9].

Для выявления уязвимостей проводится комплексное сканирование с помощью специализированных инструментов [10]. В случае с PON-роутерами акцент делается на проверку корректности реализации PON-специфичных протоколов, состояние прошивки роутера, а также аудиты заводских настроек. Кроме того, важно контролировать физическую доступность роутеров, так как PON-технологии чувствительны к подключению неавторизованных устройств в оптическую линию [11].

Также, очень важным аспектом является информирование пользователей о том, как правильно устанавливать и конфигурировать PON-роутеры, ведь во многих случаях именно от конечного пользователя зависит уровень безопасности сети [12]. Пользователи должны быть обучены использованию шифрования WPA2 [13] или WPA3 на своих беспроводных сетях, изменению стандартных паролей доступа и регулярному обновлению встроенного программного обеспечения роутера [14]. Это важно, так как многие уязвимости становятся известными после релиза оборудования, и производители обычно выпускают обновления для их устранения [15].

Регулярная ревизия и аудит конфигураций PON-роутеров также критически важны. Настройки по умолчанию могут быть потенциально уязвимы и должны

быть скорректированы для соответствия лучшим практикам безопасности [16]. Специалисты по безопасности должны проверять такие моменты, как отключение ненужных служб и портов, настройку фильтрации MAC-адресов [17], а также реализацию сегментации сети для ограничения широковещательного трафика в сетях PON.

Управление учетными данными и контроль доступа к устройствам PON являются жизненно важными, чтобы предотвратить несанкционированный доступ [18]. Это включает в себя использование инструментов управления паролями и реализацию двухфакторной аутентификации для административного доступа к роутерам.

Когда возникает подозрение об уязвимости или после обнаружения инцидента, должны быть активированы процедуры реагирования на инциденты, которые включают идентификацию, содержание, исследование, устранение уязвимостей и восстановление после атак [19]. Документирование и усвоение уроков из инцидентов позволяет улучшать процессы и предотвращать будущие угрозы.

В магистерской диссертации будет рассмотрена реализация сканера прошивок для оптических роутеров, схема, которого изображена на (рис. 1). Данный инструмент станет шагом к превентивной защите, позволяя оперативно выявлять и устранять потенциальные риски до момента их реализации злоумышленниками. Разработка такого сканера будет полагаться на исследование существующих уязвимостей, сочетая в себе последние наработки в области безопасности, что поможет корпоративным и частным сетям бережно заботиться о своей безопасности.

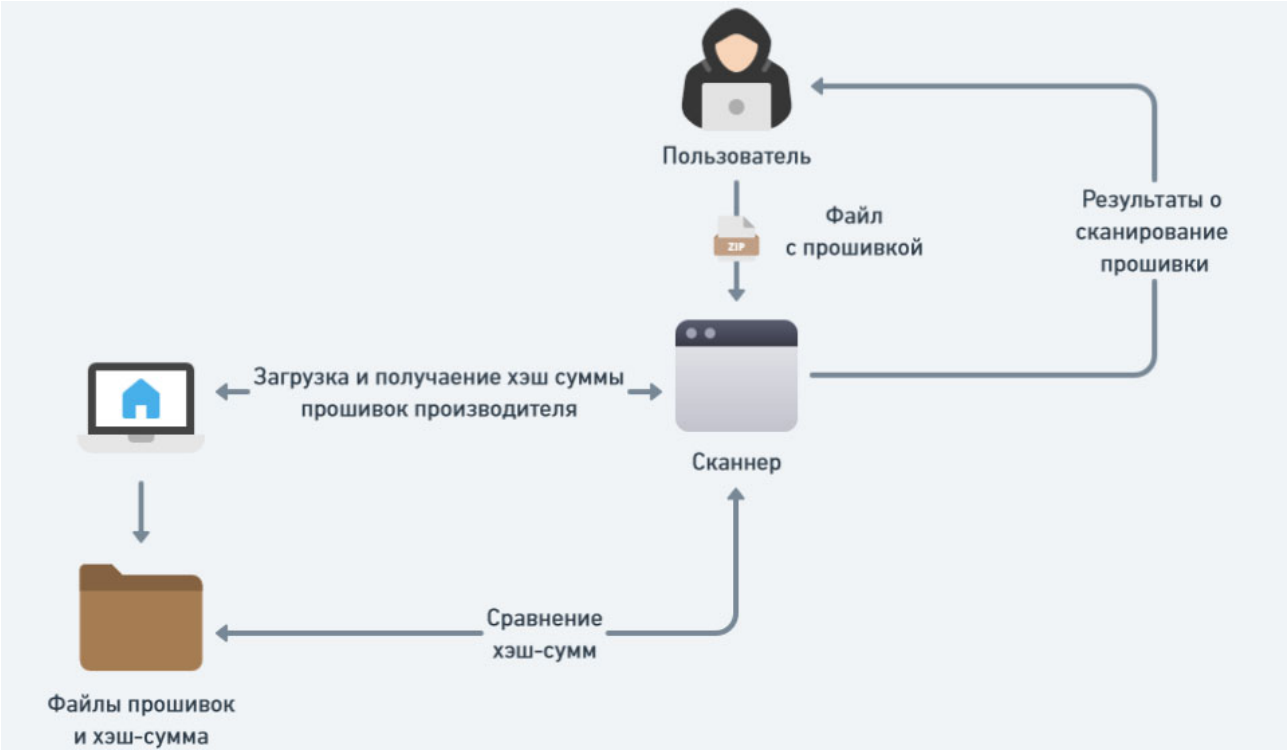

Рис. 1. Схема работы сканера

Проект также предполагает анализ требований к безопасности оптических сетевых устройств, разработку алгоритма работы сканера. Интеграция сканера в существующие системы управления безопасностью сети обеспечит непрерывный мониторинг, актуализацию данных о безопасности и повышение уровня реагирования на угрозы [20].

Заключение

Исследование и устранение уязвимостей в сетевых устройствах, особенно в PON-роутерах, играют критическую роль в укреплении информационной безопасности, ввиду их важности в обеспечении стабильной работы инфраструктуры. Эти устройства требуют особого внимания и разработки специализированных подходов к их анализу и защите. Применение рекомендуемых мер и инструментов, таких как те, что предложены OWASP, вкупе с обучающими программами, существенно повышает безопасность сетей, опирающихся на PON-технологии.

Исследование безопасности прошивок оптических роутеров имеет значительный научный и практический потенциал, так как оно направлено на решение актуальной проблемы уязвимости сетевых устройств, на которых основана большая часть интернет-инфраструктуры. Научный задел включает в себя теоретический анализ существующих типов атак на PON-роутеры, а также разработку методологии аудита их программного обеспечения. Исследование также вносит вклад в практическое применение, предоставляя инструменты и процедуры для непрерывной оценки и управления рисками в сфере сетевой безопасности.

Оригинальность предложенного сканера заключается в комбинации аудита конкретной категории устройств (PON-роутеров) с учетом их уникальных особенностей и протоколов.

Итоговым вариантом сканера будет являться консольная утилита, она позволит сетевым администраторам и специалистам по безопасности сравнивать установленную на роутерах прошивку с эталонной версией, а также проверять ее на наличие известных и потенциально новых уязвимостей. Предусмотрена возможность обнаружения заранее подготовленных скрытых угроз, таких как бэкдоры, шеллы или ботнеты.

В заключение работы, по результатам магистерской диссертации и реализации сканера прошивок оптических роутеров, планируется, что он станет значимым вкладом в общую схему защиты сетевой инфраструктуры и поспособствуют повышению уровня информационной безопасности, как на локальном, так и на глобальном уровнях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кодиров Ф. Э. Технология GPON / Ф. Э. Кодиров, В. Г. Ачилова // Математическое и информационное моделирование: сб. статей. – Тюмень, 2018. – С. 176-181.

2. Халиулин А. Ю. Технология GPON и её практическое применение // Сборник конференций НИЦ социосфера: сб. статей / А. Ю. Халиулин – Новосибирск, 2013. – С. 47-49.

3. Шубин В. В. Информационная безопасность волоконно-оптических систем. - / В. В. Шубин – Саров, ФГУП «РФЯЦ-ВНИИЭФ», 2015. – 257 с.

4. Кодиров Ф. Э. Развитие локальной сети на основе технология GPON. - Текст: непосредственный / Ф. Э. Кодиров, Ж. Э. Нематов // Инновации в технологиях и образовании:

Сборник статей участников XII Международной научно-практической конференции. Том 2. 2019 Издательство: Кузбасский государственный технический университет имени Т.Ф. Горбачева (Кемерово)сб. статей. –2019. – С. 288-291.

5. Казарин О. В. Безопасность программного обеспечения компьютерных систем. - / О. В. Казарин. – М.: Московский государственный университет леса, 2003. – 212 с.

6. OWASP [Электронный ресурс]. URL: https://owasp.org/about/

7. OWASP IoT [Электронный ресурс]. URL: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

8. ГОСТ Р Защита информации. Мониторинг информационной безопасности. Общие положения. Проект [Электронный ресурс]: Веб-сайт / ФСТЭК России. - Режим доступа: https://fstec.ru/tk-362/standarty-tk362/303-proekty/1896-proekt-natsionalnogo-standarta-gost-r-4

9. CERT [Электронный ресурс]. URL: https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team

10. OWASP ZAP [Электронный ресурс]. URL: https://habr.com/ru/companies/first/articles/709586/

11. Способ защиты информации в ВОЛС на основе оптического зашумления. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/sposob-zaschity-informatsii-v-vols-na-osnove-opticheskogo-zashumleniya

12. Построение пассивной оптической сети – PON [Электронный ресурс]. URL : https://eltexcm.ru/novosti-i-statji/stati/xpon/postroenie-pon.html

13. Уязвимость протокола WPA2 [Электронный ресурс]. URL: https://wifi-solutions.ru/uyazvimost-protokola-wpa2-kak-zashchitit-wi-fi-ot-vzloma/

14. Wi-Fi становится безопаснее [Электронный ресурс]. URL: https://habr.com/ru/articles/424925/

15. Что такое CVE и какие угрозы там хранятся? [Электронный ресурс]. URL: https://habr.com/ru/companies/pvs-studio/articles/678410/

16. Исследование семейство технологий pon и анализ проблем резервированиЯ [Электронный ресурс]. URL: https://elar.urfu.ru/bitstream/10995/36233/1/ittsm-2016-12.pdf

17. Фильтрация MAC-адресов [Электронный ресурс]. URL: https://encyclopedia.kaspersky.ru/glossary/mac-filtering/

18. Аутентификация [Электронный ресурс]. URL: https://sendpulse.com/ru/support/glossary/authentication

19. Инциденты [Электронный ресурс]. URL: https://docs.usergate.com/incidenty-401/

20. Сотикова Д.В. Применение сетевых сканеров безопасности в локальных сетях учреждений уголовно-исполнительной системы / Сотикова Д.В., Корчагина Е.В., Андреева Н.А. // Воронежский институт ФСИН России: сб. статей – Воронеж: 2021. – С 234-236.