Похоже, компания решила более ответственно подойти к вопросам безопасности

Не успели мы опубликовать вчерашнюю новость о том, что исследователи Watchtower Labs обвинили компанию в QNAP Systems Inc. — производитель сетевых устройств и решений для хранения данных; Компания была основана в 2004 году как дочерняя компания IEI Integration Corporation.

 QNAP специализируется на аппаратных системах для обмена файлами, управления хранилищами, виртуализации и облачных сервисах, а также на приложениях для наблюдения для дома и бизнеса. Компания предлагает ряд продуктов для различных сред, от SOHO до компаний масштаба предприятия." data-html="true" data-original-title="QNAP" >QNAP в медленном реагировании на ответственное раскрытие уязвимостей, уже сегодня стало известно, что NAS, или сетевое хранилище данных, позволяет получать доступ к файлам с любого компьютера или мобильного устройства, если оно подключено к той же сети. По сути, NAS соединяет несколько устройств хранения (например, жестких дисков) в сеть." data-html="true" data-original-title="NAS" >NAS-гигант, похоже, встал на путь истинный, опубликовав сразу 5 исправлений для затронутых операционных систем QTS и QuTS hero.

Среди исправленных уязвимостей:

Все уязвимости требуют для эксплуатации наличия учётной записи на устройствах NAS, все были исправлены в обновлениях QTS 5.1.7.2770 и QuTS hero h5.1.7.2770. Обнаруживший и сообщивший о проблемах исследователь Алиц Хаммонд из watchTowr Labs — это центр экспертизы по наступательной безопасности. В блоге центра публикуются результаты исследований, анализы уязвимостей, а также методики этичного хакинга, позволяющие различным компаниям укреплять свою кибербезопасность." data-html="true" data-original-title="watchTowr Labs" >WatchTowr Labs получил признание от компании QNAP за свои усилия.

«Уязвимость CVE-2024-27130 связана с небезопасным использованием функции «strcpy» в функции «No_Support_ACL», используемой в скрипте «share.cgi» для обмена медиа с внешними пользователями», — говорится в заявлении QNAP. «Для эксплуатации этой уязвимости требуется действительный параметр SSID, который генерируется при обмене файлами с NAS-устройствами».

QNAP отметила, что все версии QTS 4.x и 5.x имеют включённую функцию ASLR, затрудняющую эксплуатацию данной уязвимости.

Обновления были выпущены через четыре дня после того, как сингапурская компания

по кибербезопасности обнародовала информацию о 15 уязвимостях, включая четыре бага, которые могли быть использованы для обхода аутентификации и выполнения произвольного кода.

Уязвимости под идентификаторами CVE-2023-50361 — CVE-2023-50364 были исправлены QNAP 25 апреля 2024 года. Однако, компания ещё не выпустила исправления для CVE-2024-27131, которую WatchTowr описал как «спуфинг логов через «x-forwarded-for», позволяющий записывать загрузки с произвольного источника».

В то же время QNAP утверждает, что CVE-2024-27131 не является уязвимостью, а представляет собой «дизайнерское решение», требующее изменения спецификаций интерфейса QuLog Center. Как бы то ни было, данное «решение» планируется исправить в QTS 5.2.0.

Подробности о четырёх других уязвимостях пока не раскрываются, однако уже известно, что одна из них получила идентификатор CVE и будет исправлена в ближайшем обновлении.

Эксперты WatchTowr заявили, что были вынуждены опубликовать информацию об уязвимостях после того, как QNAP не устранила их в течение 90-дневного срока раскрытия информации. При том, что компания несколько раз просила отсрочку в публикации общедоступного отчёта.

В ответ на критику QNAP выразила сожаление по поводу координационных проблем и обязалась выпускать исправления для критических уязвимостей в течение 45 дней, а для уязвимостей средней опасности — в течение 90 дней.

«Приносим извинения за любые неудобства и стремимся постоянно улучшать наши меры безопасности», — добавили в компании. «Наша цель — тесно сотрудничать с исследователями по всему миру для обеспечения наивысшего уровня безопасности нашей продукции».

С учётом того, что уязвимости в устройствах QNAP NAS ранее использовались атакующими, пользователям рекомендуется как можно скорее обновить свои системы до последних версий QTS и QuTS hero для предотвращения потенциальных угроз.