Pavel Stepanov Follow
Apr 28, 2020 · 6 min read

Анализ безопасности роутера Smart Box

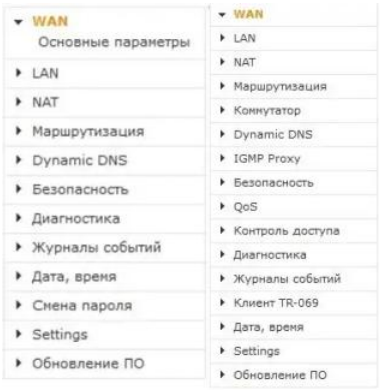
Здравствуй, дорогой читатель!

Сегодня мы начнем с того, что в один момент я решил вместо того, чтобы тренироваться на уязвимых машинах, протестировать свой собственный Wi-Fi роутер на уязвимости, который я получил еще в 2015 году. Тогда был очень популярный тариф у Билайна, когда вместе с подключением интернета, в аренду за 1 рубль шел и сам Wi-Fi роутер, который я и решил протестировать.

Роутер Smart Box, последняя версия прошивки — 2.0.38 (Релиз прошивки 2017 года), с тех пор, обновлений не поступало.

Начало

По умолчанию у роутера есть 2 учетные записи admin и SuperUser, об этом мало кто знает, но об этом есть информация в открытых источниках. Пароль от пользователя SuperUser, это серийный номер роутера и его можно узнать в настройках во вкладке “Расширенные настройки > Информация” или на наклейке под роутером. Соответственно у пользователя SuperUser больше возможностей по настройке роутера.



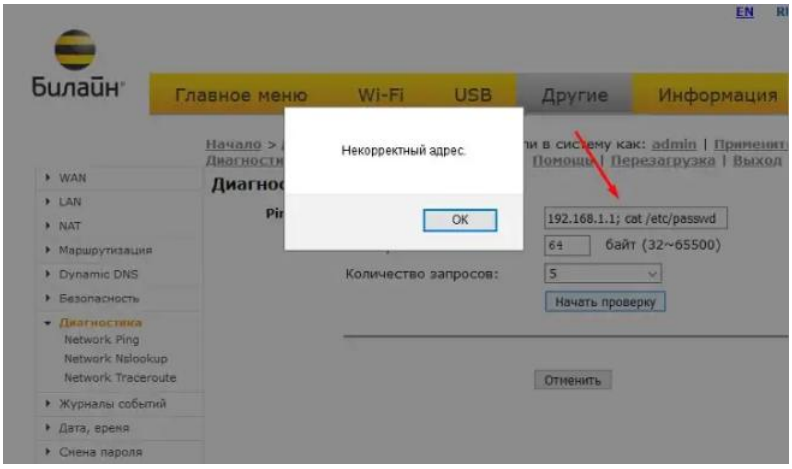
Пользователь admin/SuperUser

У роутера есть несколько видов учетных записей “Пользователь, администратор и производитель”, соответственно у них разные привилегия в плане конфигурации роутера и это мы берем на заметку.

OS Command Injection

Да, у роутера есть уязвимость внедрения команд.

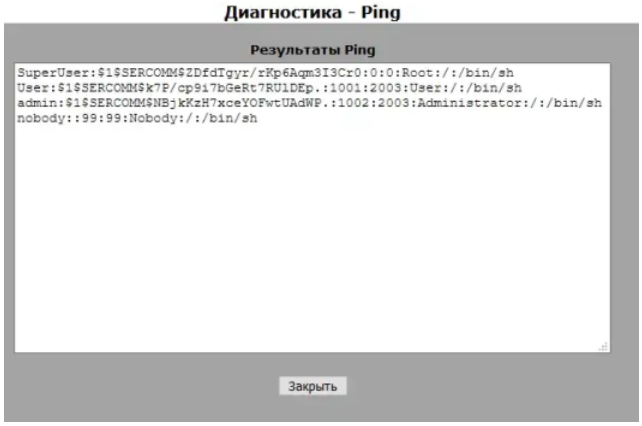
Сперва мы авторизовываемся и переходим в “Расширенные настройки > Другие > Диагностика” и мы можем осуществить Ping, nslookup и traceroute, с помощью встроенных функции роутера. Попробуем выполнить ping и тем самым выполнить другую команду.



Защита на стороне клиента

Как мы видим, нас предупреждают что адрес некорректный, но эта з... ет только на стороне клиента. Если мы перехватим запрос и изменим его, то мы обойдем эту защиту. А делать я это буду с помощ... ата Burp Suite pro.

Перехватываем запрос и изменяем его



Результат

Как мы видим, вместо пинга выполнилась совершенно другая команда, которую мы указали, когда перехватывали запрос. Тут мы видим, что у роутера есть 3 учетные записи (SuperUser, User, admin), пользователя User я создал сам. По умолчанию будет только 2 пользователя (SuperUser и admin). Вот с помощью этой уязвимости, я узнал про пользователя SuperUser, тогда я был очень удивлен и мне стало очень интересно.

Данная уязвимость присутствует и в nslookup и traceroute и эксплуатируется она таким же способом, с помощью перехвата запроса. Ниже прикрепляю PoC видео с эксплуатацией уязвимостей.

Ping

Nslookup

Traceroute

Помните в начале мы брали на заметку, что есть 3 типа учетных записей? Так вот, независимо от типа учетной записи, команды выполняются с привилегиями SuperUser, что дает нам больше возможностей. И да, уязвимость присутствует в любой типе учетной записи (Пользователь, администратор и производитель).

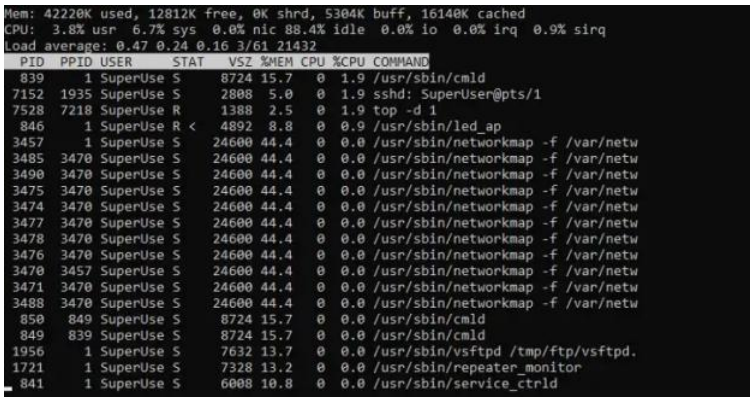
Уязвимые сервисы

У роутера есть 3 сервиса “OpenSSH 5.2, FTP vsftpd 3.0.2 и Samba 3.0.22”. Сервисы старых версии и в них найдено множество уязвимостей за все время. Чтобы вы понимали, на момент написания статьи, последние версии сервисов (OpenSSH 8.2, FTP vsftpd 3.0.3 и Samba 4.12.0). Я отобрал пару эксплойтов к этим сервисам для теста и начнем мы по порядку.

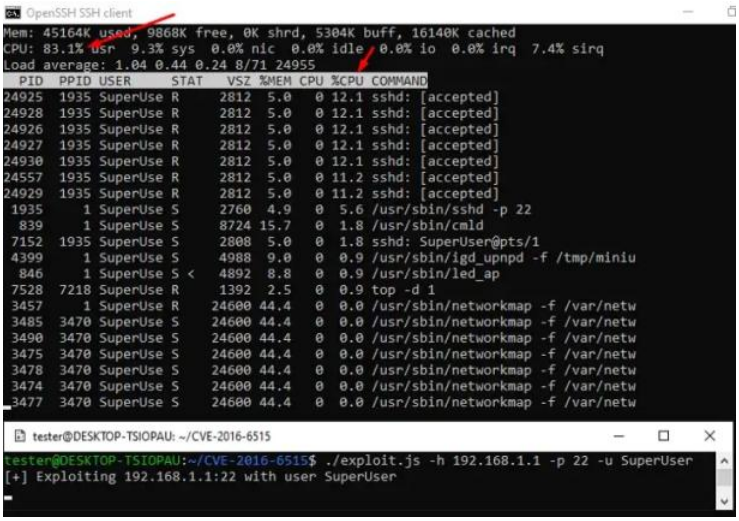
OpenSSH (5.2)

Уязвимость CVE-2016–6515 позволяет вызвать отказ в обслуживании DoS.

Я авторизовываюсь в системе роутера по SSH и с помощью команды top мониторим нагрузку на процессор и смотрим на поле (CPU) и эксплуатируем уязвимость.



В обычном состояний



После эксплуатации уязвимости

В итоге веб-страницы могут долго грузится и даже в какой то момент роутер может намертво зависнуть и даже уйти в перезагрузку. Но у меня был забавный случай, когда во время эксплуатации этой уязвимости, мой компьютер ушел в перезагрузку с синим экраном смерти (Грустный смайлик), это было очень неожиданно и странно:D

Ниже прикладываю PoC видео с эксплуатацией этой уязвимости.

Эксплуатация CVE-2016-6515

Samba (3.0.22)

Уязвимость smb loris, которая позволяет вызвать отказ в обслуживании DoS. Данную уязвимость можно эксплуатировать с помощью metasploit, находиться она по пути “auxiliary/dos/smb/smb_loris”. В итоге роутер уйдет в перезагрузку.

Ниже прикладываю PoC видео с эксплуатацией уязвимости.

FTP (vsftpd 3.0.2)

Уязвимость CVE-2015–1419, позволяет обойти ограничения доступа. Эксплоит к сожалению я не нашел, но тоже имеет место быть.

https

Да, у роутера есть возможность включения безопасного соединения. Как я понял, используется протокол шифрования SSL 2.0 или 3.0 и сертификат является самоподписанным, что вполне нормально для локальных роутеров. И в плане безопасности, SSL уже давно устарел и небезопасен. Сейчас используются более безопасные варианты, как TLS 1.3

Другие слабые места

Во время аутентификации в роутере, логин и пароль кодируются в base64, что не составляет особого труда декодировать их. С учетом того что по умолчанию не используется протокол https, для зашифрованного соединения, то кодировка логина и пароля, это хоть какая то защита. Лучше пусть данные передаются в кодированном состоянии, чем полностью в открытом. Скажу честно, в первое время, меня этот момент завел в заблуждения и только через некоторое время я понял, что данные кодируются.

Логин и пароль передаются в кодированном состоянии

После декодирования

Ниже прикладываю PoC видео с декодированием.

Base64 decode

Злоумышленникам не составит особо труда прослушать сеть и с помощью анализа трафика, выявить логин и пароль и декодировать их.

Обращение в Билайн

Изначально я обратился к ним с помощью онлайн-чата и они порекомендовали мне позвонить и там задать все вопросы, что я и сделал.

Задал я всего лишь пару вопросов и вот какой итог: Роутер Smart box больше не актуален и обновления больше на него выходить не будут. И как я писал в самом начале, он перестал обновляться с 2017 года, вот тогда и было его последнее обновление. Как упомянул оператор Алексей (Если ты это читаешь, большой привет тебе) что роутер Smart box one до сих пор поддерживается и если в нем кто нибудь найдет уязвимость, то может смело звонить и информацию передадут в службу безопасности. Как я понял, Smart box one это следующая модель после Smart box.

Итоги

Роутер сам по себе хороший, но в плане безопасности он к сожалению устарел. Если им и пользоваться, то рекомендуется отключить такие службы как SSH,FTP и Samba, так как они старых версий и в них найдено много уязвимостей и пользоваться ими небезопасно, особенно в глобальной сети. Будет еще лучше, сменить роутер на более новую модель (Не важно от какого вендора) который будет поддерживаться в плане обновлений безопасности.

Напоследок зайдем в Shodan и посмотрим, сколько доступно роутеров Smart box в глобальной сети.

Как мы видим, всего найдено 79 устройств и это еще с учетом того, что у меня аккаунт бесплатной версии, без подписки. Соответственно с подпиской будет куда больше результатов и возможностей. Так же тут стоит учесть, что в глобальной сети доступно Smart box роутеров разных моделей, как мы видим справа. Так вот, большинство Smart box роутеров (Не важно от модели роутера), используют те же самые версии уязвимых сервисов, о которых я писал выше и доступны они в глобальной сети, а это предоставляет угрозу безопасности.

Уязвимости OS Command Injection присвоен CVE идентификатор “CVE-2020-12246”.

Под конец статьи, я бы хотел дать пару советов читателям:
1. Обновляйте прошивки своих роутеров
2. Отключайте неиспользуемые вами службы
3. Следите за активностью в вашей сети
Безопасность роутера действительно важна, ведь к нему подключается множество устройств, а эти устройства могут стать целями злоумышленников для компрометации.

Beeline Pentest Information Security Vulnerability Smart Box