Публикации

НАЗАД

Recognizing local privilege escalation in ABBYY FineReader

19.02.2020

Статья

I continue my series about Windows applications privilege escalation discovery. Previously on this series: Steam (CVE-2019-14743, CVE-2019-15316, CVE-2019-17180) and Origin (CVE-2019-19247, CVE-2019-19248). But today it is not about a gaming launcher, but a desktop application ABBYY FineReader.

TL;DR: I am going to tell how you can escalate privileges from user to NT AUTHORITY\SYSTEM in 10 minutes, using the licensing component of ABBYY FineReader. This vulnerability was assigned CVE-2019-20383, here is a link to ABBYY website: https://support.abbyy.com/hc/ru/articles/360008536920-%D0%98%D1%81%D1%82%D0%BE%D1%80%D0%B8%D1%8F

Мы используем файлы cookie. Это позволяет нам анализировать взаимодействие посетителей с сайтом и делать его лучше. К сайту подключен сервис веб-аналитики Яндекс.Метрика, использующий файлы cookie. Вы всегда можете отключить файлы cookie в настройках вашего браузера. Продолжая пользоваться сайтом, вы даете Согласие на обработку персональных данных в соответствии с нашей Политикой обработки персональных данных.

OK

grabbed my attention. The service readed something from it, wrote something to it. It looked like an interesting testing candidate. Let’s look at the «C:\ProgramData\ABBYY\FineReader\15\Licenses» folder. This folder has «All - FullControl» legacy ACL from its parent directory «C:\ProgramData\ABBYY\FineReader\15» , which means that it is possible to remove its contents, including «Licensing.cnt».

The service, on discovering that the file was removed, tries to create it in its own strange way. It creates a file named like «tmpXXXX-YYYYYYYYY.tmp», writes some data to it, then renames it to «Licensing.cnt».

Here is a ProcMon log, where this operation is performed twice



For the first time it occurs at 20:36, then at 20:46. Between this timestamps I removed the file again, so it could be created one more time.

Мы используем файлы cookie. Это позволяет нам анализировать взаимодействие посетителей с сайтом и делать его лучше. К сайту подключен сервис веб-аналитики Яндекс.Метрика, использующий файлы cookie. Вы всегда можете отключить файлы cookie в настройках вашего браузера. Продолжая пользоваться сайтом, вы даете Согласие на обработку персональных данных в соответствии с нашей Политикой обработки персональных данных.

Summarizing this part – any user can remove «C:\ProgramData\ABBYY\FineReader\15\Licenses\Licensing.cnt» file, then, in cycle, he can constantly look for contents in «C:\ProgramData\ABBYY\FineReader\15\Licenses» folder and at some point discover a file named «tmpXXXX_YYYYYYYYY.tmp» there. A user is now prepared — after removing the file he will know exactly at what time and with what name the file will be created next time.

Now we are going to play with symlinks

Creating symlink from file to file requires administrative rights. But the requirement could be bypassed. Let's see how we can create symlink from "C:\abc\1" to "C:\def\2".

First, let's create an NTFS reparse point (sometimes called NTFS mount point) from "C:\abc" directory to "\RPC Control\". "\RPC Control\" is not a regular directory, it can't be viewed by explorer. It's a system object directory, which stores, for example, named mutexes, events and other similar objects. It's not clear, why redirection with NTFS reparse point works with it, most likely because similar abstractions are used for directories in filesystem and object directories. There are two requirements for reparse point creation: a source directory must be empty and a user must have write permission on the dir.

It is possible to create symlink from object directory to file without administrative permissions. Let's create symlink "\RPC Control\1" <-> "C:\def\2". So all operations on "C:\abc\1" will be redirected to "C:\def\2".

Originally the process looks like this:

Мы используем файлы cookie. Это позволяет нам анализировать взаимодействие посетителей с сайтом и делать его лучше. К сайту подключен сервис веб-аналитики Яндекс.Метрика, использующий файлы cookie. Вы всегда можете отключить файлы cookie в настройках вашего браузера. Продолжая пользоваться сайтом, вы даете Согласие на обработку персональных данных в соответствии с нашей Политикой обработки персональных данных.

If we know the exact moment of the next attempt to perform this operation, we can create the following symlinks (I skip the current directory name, which is «C:\ProgramData\ABBYY\FineReader\15\Licenses\»):

tmpXXXX_YYYYYYYYA.tmp <-> C:\test\l1\proxy

tmpXXXX_YYYYYYYYB.tmp <-> C:\test\l1\proxy

tmpXXXX_YYYYYYYYC.tmp <-> C:\test\l1\proxy

…

tmpXXXX_YYYYYYYYZ.tmp <-> C:\test\l1\proxy

Where YYYYYYYYA, YYYYYYYYB, YYYYYYYYC, … YYYYYYYYZ are different timestamps in YYYYYYYY + 10 minutes area (is case the timestamp is running a little bit late).

Мы используем файлы cookie. Это позволяет нам анализировать взаимодействие посетителей с сайтом и делать его лучше. К сайту подключен сервис веб-аналитики Яндекс.Метрика, использующий файлы cookie. Вы всегда можете отключить файлы cookie в настройках вашего браузера. Продолжая пользоваться сайтом, вы даете Согласие на обработку персональных данных в соответствии с нашей Политикой обработки персональных данных.

renaming already after following a new symlink. Thus, instead of renaming, for example «tmpXXXX_YYYYYYYYC.tmp» to «Licensing.cnt», it will rename (replace) «C:\test\l2\payload» to «C:\target\path». In fact, we can place any file with any content in any directory with NT AUTHORITY\SYSTEM permissions.

Schematically it looks like this:



Мы используем файлы cookie. Это позволяет нам анализировать взаимодействие посетителей с сайтом и делать его лучше. К сайту подключен сервис веб-аналитики Яндекс.Метрика, использующий файлы cookie. Вы всегда можете отключить файлы cookie в настройках вашего браузера. Продолжая пользоваться сайтом, вы даете Согласие на обработку персональных данных в соответствии с нашей Политикой обработки персональных данных.

According to ABBYY, at this moment the vulnerability is fixed.

Timeline:

25.11.2019 – vulnerability discovery
26.11.2019 – requested a security contact from vendor
26.11.2019 – sent the vulnerability report to vendor
09.12.2019 – vulnerability is confirmed by vendor
10.01.2020 – vulnerability is fixed
22.01.2020 – vulnerability is assigned CVE-2019-20383
19.02.2020 – this article publication

About author

Vasily Kravets, Lead Expert

ВСЕ ПУБЛИКАЦИИ →

Наши услуги

Мы используем файлы cookie. Это позволяет нам анализировать взаимодействие посетителей с сайтом и делать его лучше. К сайту подключен сервис веб-аналитики Яндекс.Метрика, использующий файлы cookie. Вы всегда можете отключить файлы cookie в настройках вашего браузера. Продолжая пользоваться сайтом, вы даете Согласие на обработку персональных данных в соответствии с нашей Политикой обработки персональных данных.

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

Мы используем файлы cookie. Это позволяет нам анализировать взаимодействие посетителей с сайтом и делать его лучше. К сайту подключен сервис веб-аналитики Яндекс.Метрика, использующий файлы cookie. Вы всегда можете отключить файлы cookie в настройках вашего браузера. Продолжая пользоваться сайтом, вы даете Согласие на обработку персональных данных в соответствии с нашей Политикой обработки персональных данных.

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

«Перспективный мониторинг» — один из лидеров российского рынка коммерческих SOC, исследования защищённости и расследования инцидентов, а также разработчик киберполигона Ampire и других собственных продуктов в области информационной безопасности.

Телефон
+7 (495) 737-61-97

Почта
info@amonitoring.ru

Адрес
127273, Россия, Москва, ул. Отрадная, д. 2Б, стр. 1

Написать нам

ФИО*

+7 (___) ___-__-__

Должность

Название организации*

Электронная почта*

Текст сообщения

Нажимая кнопку «отправить», я подтверждаю ознакомление и даю Согласие на обработку персональных данных, в соответствии с Политикой обработки персональных данных, а также даю свое согласие ООО «Яндекс» на обработку данных, необходимых для работы Yandex SmartCaptcha в соответствии с Политикой конфиденциальности Яндекс.

Я согласен на получение новостных и информационных рассылок.

Мы используем файлы cookie. Это позволяет нам анализировать взаимодействие посетителей с сайтом и делать его лучше. К сайту подключен сервис веб-аналитики Яндекс.Метрика, использующий файлы cookie. Вы всегда можете отключить файлы cookie в настройках вашего браузера. Продолжая пользоваться сайтом, вы даете Согласие на обработку персональных данных в соответствии с нашей Политикой обработки персональных данных.

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Мы используем файлы cookie. Это позволяет нам анализировать взаимодействие посетителей с сайтом и делать его лучше. К сайту подключен сервис веб-аналитики Яндекс.Метрика, использующий файлы cookie. Вы всегда можете отключить файлы cookie в настройках вашего браузера. Продолжая пользоваться сайтом, вы даете Согласие на обработку персональных данных в соответствии с нашей Политикой обработки персональных данных.