Сообщить об инциденте
Поиск Найти
+7 495 737-61-97
info@amonitoring.ru

07.07.2020

Local privilege escalation in Dr.Web Security Space

Another article about local privilege escalation. Previously on this series: Steam (CVE-2019-14743, CVE-2019-15316, CVE-2019-17180), Origin (CVE-2019-19247, CVE-2019-19248), ABBYY FineReader (CVE-2019-20383).

This is a short paper with technical details of exploitation. A little bit more information about research in Russian article — https://habr.com/ru/509592/.

Video of exploitation with time-based comments:

Demo stand for exploitation is Windows 10 x64, active user has no administrative privileges.

0:00-0:12 Open Windows console and check that active user has no administrative privileges

0:12-0:24 Show actual version of installed Dr.Web Security Space

0:24-0:29 There is a file drweb_eop_upd_dll.dll at user's desktop (this file and its source code were attached to report for vendor)

0:29-0:34 Show that the directory C:\ProgramData\Doctor Web\Updater\etc contains only 3 files.

0:34-0:47 Copy drweb_eop_upd_dll.dll twice. One is renamed to version.dll, another to cryptui.dll

0:47-0:56 Copy an executable file C:\Program Files\Common Files\Doctor Web\Updater\drwupsrv.exe to the directory with dlls.

0:56-1:00 Start the executable.

When drwupsrv.exe starts, it loads version.dll from its startup directory. The dll creates file C:\ProgramData\Doctor Web\Updater\etc\drwupsrv.xml.new. A user is allowed to create files and folders at path C:\ProgramData due to a special permissive ACL. When the user is to create a file manually (for example, from explorer's context menu), it seems that the Dr.Web Security Space mechanisms restricts the operation in that directory. During the attack, all operations are requested from legit Dr.Web executable called drwupsrv.exe, so the restriction might be bypassed.

1:00-1:22 Show created file and its content. This is the same file as C:\ProgramData\Doctor Web\Updater\etc\drwupsrv.xml, but all paths are changed to the user-controlled folder (C:\Users\User\Desktop\dwtest).

1:22-2:00 Nothing happens (awaiting auto-update that happens every 30 minutes by default).

2:00-2:14 It seems that updater reads created file as a config and tries to update product in the user-controlled folder. Since there is no anything related to product, updater starts to copy whole product to the folder.

Among the files, there is a file named dwservice.exe (placed at user-controlled folder), that starts during updating process with NT AUTHORITY\SYSTEM privilege. The file loads cryptui.dll that was planted at the very beginning. The dll just spawns an interactive console. Show rights via whoami command.

Timeline:

15.05.2020 – Ask for vendor's security-contact

20.05.2020 – Vendor permits send report due to support ticket

20.05.2020 – Report sent

14.06.2020 – Vendor says that fix for Dr.Web Security Space 12 are available. Request time for fix Dr.Web Security Space 11.

07.07.2020 – Vendor says that all fixes are released.

About author

Vasily Kravets, Lead Expert

mailto:xi-tauw@xi-tauw.info

mailto:Vasily.Kravets@amonitoring.ru

https://twitter.com/PsiDragon

https://t.me/xitauw

Теги:
Dr Web lpe
Поделиться статьей в:

Рекомендуемые статьи

О нас

- Компания
- Вакансии
- Контакты

Услуги

- Центр мониторинга компьютерных атак
- Разработка правил Snort IDS
- Внедрение процедур безопасной разработки ПО
- Расследование компьютерных инцидентов
- Соответствие требованиям по ИБ
- Анализ защищённости
- Пентесты
- Управление инцидентами ИБ
- ГосСОПКА

Написать нам

Имя

Email

Письмо

Введите код с картинки CAPTCHA

ОТПРАВИТЬ

2022

Как к вам обращаться?

Адрес электронной почты

Ваш вопрос, запрос или пожелание связаться с вами

*Мы не спамим и не подписываем на рассылку

Быстро ответим только с 9 до 18 по Москве.

В противном случае — на следующий день.

Введите код с картинки

Отправить