# CVE 2020-1034

Фирсов Георгий

НИЯУ МИФИ
Кафедра №42 "Криптология и кибербезопасность"
Группа М21-507

24 марта 2022

# Содержание доклада

# Общее описание

Уязвимость заключается в некорректной проверке параметров во внутренней функции ядра Windows `EtwpNotifyGuid`.
Данная функция вызывается внутри `NtTraceControl` с передачей в нее указателя на структуру типа `ETWP_NOTIFICATION_HEADER`:

```
1  typedef struct _ETWP_NOTIFICATION_HEADER {
2      ...
3      BOOLEAN ReplyRequested;     // (1)
4      ...
5      union
6      {
7          ULONGLONG ReplyHandle; // (2)
8          PVOID     ReplyObject; // (3)
9          ULONG     RegIndex;
10     };
11     ...
12 } ETWP_NOTIFICATION_HEADER, *PETWP_NOTIFICATION_HEADER;
```

# Обработка параметров в EtwpNotifyGuid

## Декомпилированный код EtwpNotifyGuid:

```
1 if (NotificationHeader->ReplyRequested == TRUE) {
2     // Processing TRUE
3     Status= EtwpCreateUmReplyObject(etwGuidEntry, &dummy,
4         &NotificationHeader->ReplyObject);
5     ...
6 }
7
8 ...
9
10 if (!NotificationHeader->ReplyRequested) {
11     // Processing FALSE
12     goto Continue;
13 }
14
15 ObfReferenceObject(NotificationHeader->ReplyHandle) // BOOM!
```

# Проблема

Тип BOOLEAN на самом деле это unsigned char:

```
1 // From ntdef.h
2 typedef unsigned char UCHAR;
3 ...
4 typedef UCHAR BOOLEAN;
```

## Следствие

В ETWP_NOTIFICATION_HEADER::ReplyRequested можно положить не только значения TRUE или FALSE.
То есть можно обойти обе проверки и передать в ObfReferenceObject произвольный адрес, значение по которому она инкрементирует.

# Маркер доступа в Windows

## Маркер доступа

Объект, описывающий контекст безопасности процесса или потока.

Маркеры доступа содержат следующие сведения:

- Идентификатор безопасности (SID) для учетной записи пользователя.
- Список привилегий пользователя или групп пользователя.
- ...

Привилегии хранятся в виде битовых флагов.

# SeDebugPrivilege и идея эксплойта

Если вызывающая сторона обладает привилегией SeDebugPrivilege, диспетчер процессов разрешает доступ *к любому процессу или потоку* с использованием NtOpenProcess или NtOpenThread *независимо от дескриптора безопасности* процесса или потока (кроме защищенных процессов).

## Идея эксплуатации:

1. Передать при помощи NtTraceControl указатель на маску привилегий в маркере доступа в уязвимую EtwpNotifyGuid, тем самым получить привилегию SeDebugPrivilege.
2. Открыть процесс svchost.exe, запустить новый процесс, используя svchost.exe как родителя.
3. Выполнить произвольный код от имени системы.

# Запуск эксплойта

Windows PowerShell

```
PS C:\Users\User\Desktop> .\exploit.exe
GetProcAddress(NtTraceControl) => 0x00000000
GetProcAddress(EtwNotificationRegister) => 0x00000000
GetProcAddress(NtQuerySystemInformation) => 0x00000000
GetProcAddress(NtQueryObject) => 0x00000000
Found current process token
Process token address: 0xFFFFB6000D143670
Editing addresses: 0xFFFFB6000D1436B2, 0xFFFFB6000D1436BA
Editing privileges...
Done editing privileges
Exploit successfully elevated to receive debug privileges
Created new process with ID 6296
```

Рис. 1: Успешный запуск нового процесса

# Запуск эксплойта

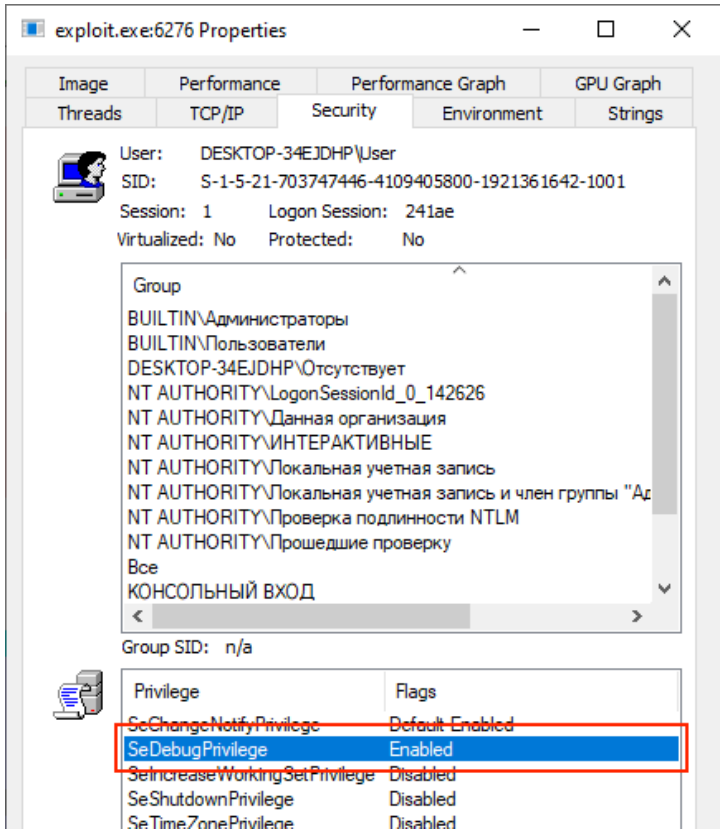


Рис. 2: Процесс эксплойта имеет привилегию `SeDebugPrivilege`

# Новый процесс

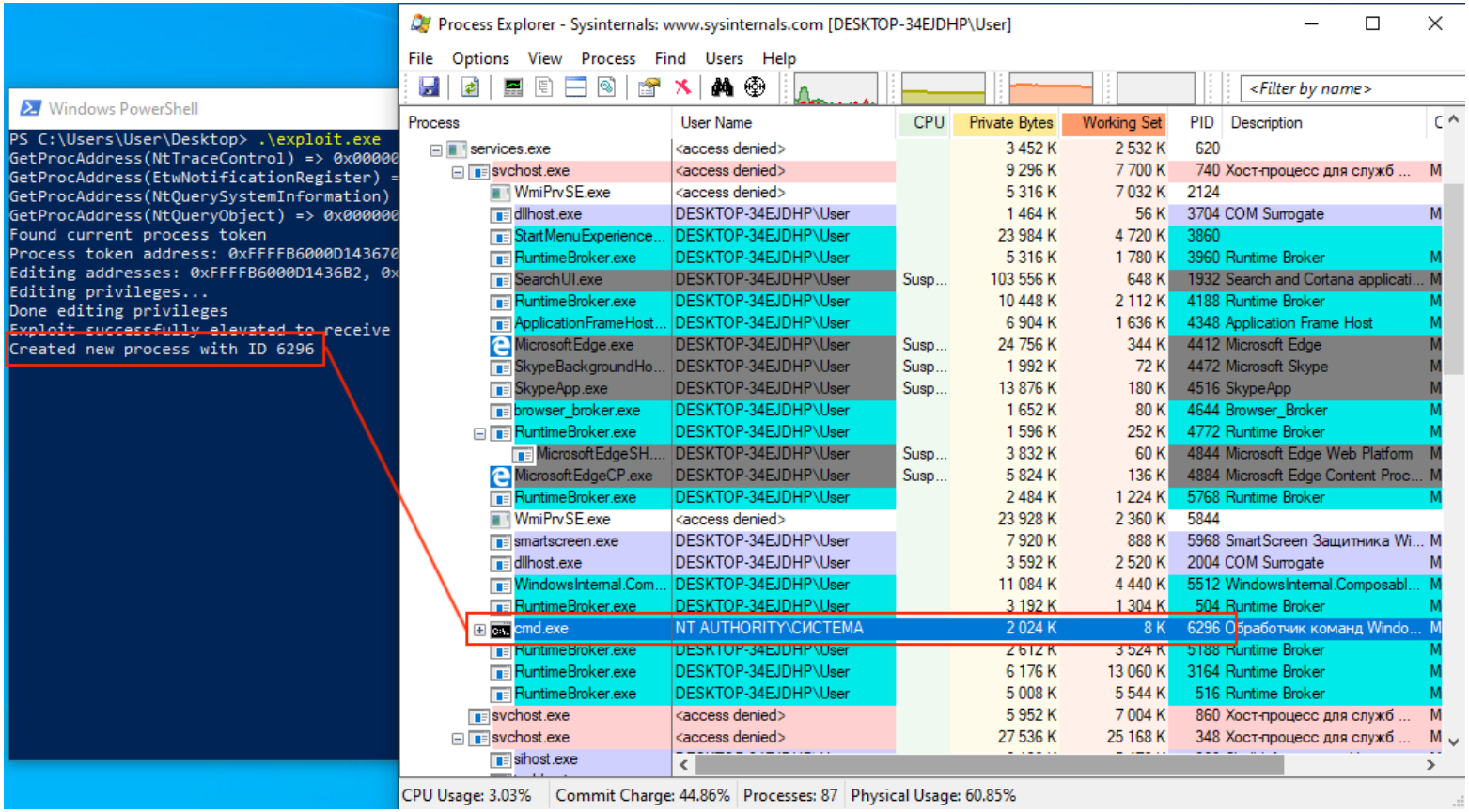


Рис. 3: Созданный процесс запущен от имени системы

# Уязвимые версии системы и меры защиты

## Уязвимые версии Windows

Все версии Windows 10 и Windows Server 2019, все сборки до 1909 включительно, а также некоторые 2004.

## Меры защиты

- Установить обновление KB4571756 от 8 сентября 2020.

# Список использованной литературы


1. Windows Kernel Elevation of Privilege Vulnerability [Электронный ресурс] : 2020. – Режим доступа: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1034. Дата обращения: 21.03.2022.
2. Руссинович М., Соломон Д., Ионеску А., Йосифович П. Внутреннее устройство Windows. 7-е изд. – СПб.: Питер, 2018. – 944 с.: ил. – (Серия "Классика computer science").