

CVE 2020-1034

Фирсов Георгий

НИЯУ МИФИ
Кафедра №42 "Криптология и кибербезопасность"
Группа M21-507

24 марта 2022



Содержание доклада

- 1 Описание уязвимости
- 2 Эксплуатация уязвимости
- 3 Уязвимые версии системы и меры защиты
- 4 Список использованной литературы



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

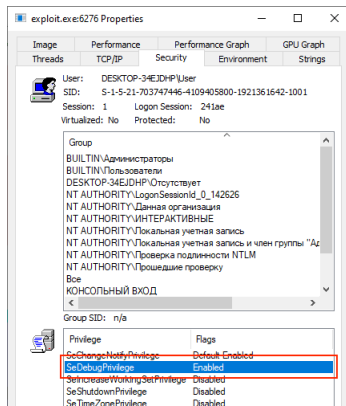


Рис. 2: Процесс эксплойта имеет привилегию SeDebugPrivilege



Новый процесс

Windows PowerShell

```
PS C:\Users\User\Desktop> .\exploit.exe
GetProcAddress(NtTraceControl) => 0x00000000
GetProcAddress(EtwNotificationRegister) =
GetProcAddress(NtQuerySystemInformation)
GetProcAddress(NtQueryObject) => 0x00000000
Found current process token
Process token address: 0x00000000143670
Editing addresses: 0x000000001436B2, 0x
Done editing privileges
Exploit successfully elevated to receive
Created new process with ID 6296
```

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-34EJHP\User]

Process	User Name	CPU	Private Bytes	Working Set	PID	Description
services.exe	<access denied>		3 452 K	2 532 K	620	
svchost.exe	<access denied>		9 296 K	7 700 K	740	Хост-процесс для служб...
WmiPrivSE.exe	<access denied>		5 316 K	7 032 K	2124	
dhost.exe	DESKTOP-34EJHP\User		1 464 K	56 K	3704	COM Surrogate
StartMenuExperience...	DESKTOP-34EJHP\User		23 984 K	4 720 K	3860	
RuntimeBroker.exe	DESKTOP-34EJHP\User		5 316 K	1 780 K	3960	Runtime Broker
SearchUI.exe	DESKTOP-34EJHP\User	Susp...	103 556 K	649 K	1932	Search and Cortana applicati...
RuntimeBroker.exe	DESKTOP-34EJHP\User		10 448 K	2 112 K	4188	Runtime Broker
ApplicationFrameHost...	DESKTOP-34EJHP\User		6 904 K	1 636 K	4348	Application Frame Host
MicrosoftEdge.exe	DESKTOP-34EJHP\User	Susp...	24 756 K	344 K	4412	Microsoft Edge
SkypeBackgroundHo...	DESKTOP-34EJHP\User	Susp...	1 992 K	72 K	4472	Microsoft Skype
SkypeApp.exe	DESKTOP-34EJHP\User	Susp...	13 876 K	180 K	4516	SkypeApp
browser_broker.exe	DESKTOP-34EJHP\User		1 652 K	80 K	4644	Browser_Broker
RuntimeBroker.exe	DESKTOP-34EJHP\User		1 596 K	252 K	4772	Runtime Broker
MicrosoftEdgeSH...	DESKTOP-34EJHP\User	Susp...	3 832 K	60 K	4844	Microsoft Edge Web Platform
MicrosoftEdgeCP.exe	DESKTOP-34EJHP\User	Susp...	5 824 K	136 K	4884	Microsoft Edge Content Proc...
RuntimeBroker.exe	DESKTOP-34EJHP\User		2 484 K	1 224 K	5768	Runtime Broker
WmiPrivSE.exe	<access denied>		23 928 K	2 360 K	5844	
smartScreen.exe	DESKTOP-34EJHP\User		7 920 K	888 K	5968	SmartScreen Защитника WI...
dhost.exe	DESKTOP-34EJHP\User		3 592 K	2 520 K	2004	COM Surrogate
WindowsInternal.Com...	DESKTOP-34EJHP\User		11 084 K	4 440 K	5512	WindowsInternal Composabl...
RuntimeBroker.exe	DESKTOP-34EJHP\User		3 192 K	1 304 K	504	Runtime Broker
cmd.exe	NT AUTHORITY\SYSTEM		2 024 K	8 K	6296	Работает команда Windo...
RuntimeBroker.exe	DESKTOP-34EJHP\User		2 512 K	3 524 K	5188	Runtime Broker
RuntimeBroker.exe	DESKTOP-34EJHP\User		6 176 K	13 060 K	3164	Runtime Broker
RuntimeBroker.exe	DESKTOP-34EJHP\User		5 008 K	5 544 K	516	Runtime Broker
svchost.exe	<access denied>		5 952 K	7 004 K	860	Хост-процесс для служб...
svchost.exe	<access denied>		27 536 K	25 168 K	348	Хост-процесс для служб...

CPU Usage: 3.03% Commit Charge: 44.86% Processes: 87 Physical Usage: 60.85%

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

- ❶ 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.
- ❷ Руссинович М., Соломон Д., Ионеску А., Йосифович П. Внутреннее устройство Windows. 7-е изд. – СПб.: Питер, 2018. – 944 с.: ил. – (Серия "Классика computer science").

