# code16

**SOBOTA, 30 STYCZNIA 2021**

## Crashing ActivePresenter

Few days ago I started learning how to record a video... and that's how I found few bugs in ActivePresenter software. Below you'll find few details. Here we go...

Today we'll start here:

I used FOE2 fuzzer with the ActivePresenter available here. Version I used was 6.1.6 (x86).

After 2 days I was able to find fe crashes, for example:

### #01 - Write Access Violation

---<cut>---

```
 CommandLine: "C:\Program Files\ATOMI\ActivePresenter\ActivePresenter.exe" C:\FOE2\sf_0ebf6f654829a47e5131e344f3b0b234-vwgocx.approj


(...)
(9a0.948): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=049b6ef8 ecx=6d6e5f23 edx=0000000c esi=3a002200 edi=049bfaf0
eip=018ff515 esp=002ee804 ebp=04a77078 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00210202
image01310000+0x5ef515:
018ff515 0106            add     dword ptr [esi],eax  ds:0023:3a002200=????????


(...)


!exploitable 1.6.0.0
HostMachine\HostUser
Executing Processor Architecture is x86
Debuggee is in User Mode
Debuggee is a live user mode debugging session on the local machine
Event Type: Exception
Exception Faulting Address: 0x3a002200
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Write Access Violation


Faulting Instruction:018ff515 add dword ptr [esi],eax


Exception Hash (Major/Minor): 0xf2f9f686.0x0c7eab62


 Hash Usage : Stack Trace:
Major+Minor : image01310000+0x5ef515
Major+Minor : image01310000+0x601b80
Major+Minor : image01310000+0x647d18
Major+Minor : image01310000+0x647db6
Major+Minor : image01310000+0x5ecc6c
Minor       : image01310000+0x5edee4
Minor       : image01310000+0x410da5
Minor       : MSVCR90!free+0xec
Minor       : image01310000+0x3d45f5
Minor       : image01310000+0x3d2e68
Minor       : wxmsw30u!wxMatchWild+0x20f
Minor       : wxmsw30u!wxMatchWild+0x217
Excluded    : ntdll!RtlFreeHeap+0x7e
Instruction Address: 0x00000000018ff515


Description: User Mode Write AV
Short Description: WriteAV
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - User Mode Write AV starting at image01310000+0x00000000005ef515 (Hash=0xf2f9f686.0x0c7eab62)
```

---</cut>---

### #02 - Write Access Violation

O MNIE

code16

Cody Sixteen

Wyświetl mój pełny profil

ARCHIWUM BLOGA

- ► 2022 (16)
- ▼ 2021 (37)
  - ► 12 (1)
  - ► 11 (1)
  - ► 10 (2)
  - ► 09 (3)
  - ► 08 (8)
  - ► 07 (3)
  - ► 06 (1)
  - ► 05 (7)
  - ► 04 (2)
  - ► 03 (5)
  - ► 02 (2)
  - ▼ 01 (2)
    - Crashing ActivePresenter
    - Code16 - Notes Magazine 04
- ► 2020 (62)
- ► 2019 (97)
- ► 2018 (67)
- ► 2017 (58)
- ► 2016 (63)

ETYKIETY

.net
android
binary
crackme
ctf
debug
docker
drones
enlil
FortiGate
fuzz
infrastructure
malware
notes
pentest
poc
pwn
RE
web
writeup

```
---<cut>---
CommandLine: "C:\Program Files\ATOMI\ActivePresenter\ActivePresenter.exe" C:\FOE2\sf_0ebf6f654829a47e5131e344f3b0b234-gw8d5x.approj
(...)
(ac.200): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=004d0024 ebx=04a3afe8 ecx=0018ebdc edx=01380101 esi=004d0024 edi=004d0020
eip=775a6b90 esp=0018eb94 ebp=0018eba8 iopl=0         nv up ei pl nz ac pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00210216
ntdll!RtlEnterCriticalSection+0x12:
775a6b90 f00fba3000      lock btr dword ptr [eax],0   ds:0023:004d0024=????????

(...)

!exploitable 1.6.0.0
HostMachine\HostUser
Executing Processor Architecture is x86
Debuggee is in User Mode
Debuggee is a live user mode debugging session on the local machine
Event Type: Exception
Exception Faulting Address: 0x4d0024
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Write Access Violation

Faulting Instruction:775a6b90 lock btr dword ptr [eax],0

Exception Hash (Major/Minor): 0x11f58bfd.0x6bd38f05

 Hash Usage : Stack Trace:
Major+Minor : ntdll!RtlEnterCriticalSection+0x12
Major+Minor : image013b0000+0x5ef1eb
Major+Minor : image013b0000+0x647dae
Major+Minor : image013b0000+0x5ecc6c
Major+Minor : image013b0000+0x5edee4
Minor       : image013b0000+0x410da5
Minor       : MSVCR90!free+0xec
Minor       : image013b0000+0x3d45f5
Minor       : image013b0000+0x3d2e68
Minor       : wxmsw30u!wxMatchWild+0x20f
Minor       : wxmsw30u!wxMatchWild+0x217
Excluded    : ntdll!RtlFreeHeap+0x7e
Instruction Address: 0x00000000775a6b90

Description: User Mode Write AV
Short Description: WriteAV
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - User Mode Write AV starting at ntdll!RtlEnterCriticalSection+0x0000000000000012 (Hash=0x11f58bfd.0x6bd38f05)
---</cut>---
```

Maybe you'll find it useful. ;)

The fuzzing process is now available on the short video I created. You can find it here: ;)

Cheers

Posted by code16 at 07:38

Labels: fuzz, notes, RE, writeup

Brak komentarzy:

Prześlij komentarz

Wpisz komentarz

Nowszy post    Strona główna    Starszy post

Subskrybuj: Komentarze do posta (Atom)