Windows kernel vulnerability in win32k.sys Driver

README.md

CVEXX-XX

i just found Windows kernel vulnerability in win32k.sys Driver , the bug is fixed in kb2998812 without even mentioning there was a vulnerability in win32k.sys

so it seems Microsoft fix some bugs without talks about it :)

An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode

---

https://twitter.com/R00tkitSMM (firozimaysam@gmail.com) telegram username : https://telegram.me/firozi

Exploiting this Bug is so trivial, there was multiple methods to Exploit it (for example Find ACL of winlogon.exe and Zero It)

```
win32k!HMUnlockObject:
929bc556 8bff            mov     edi,edi
929bc558 55              push    ebp
929bc559 8bec            mov     ebp,esp
929bc55b 8b4508          mov     eax,dword ptr [ebp+8]
929bc55e ff4804          dec     dword ptr [eax+4]    ds:0023:41414145=????????
929bc561 7506            jne     win32k!HMUnlockObject+0x13 (929bc569)
929bc563 50              push    eax
929bc564 e8cf3a0000      call    win32k!HMUnlockObjectInternal (929c0038)
929bc569 5d              pop     ebp
929bc56a c20400          ret     4


2: kd> !analyze -v
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

Unknown bugcheck code (0)
Unknown bugcheck description
Arguments:
Arg1: 00000000
Arg2: 00000000
Arg3: 00000000
Arg4: 00000000

Debugging Details:
```

```
------------------

PROCESS_NAME:  0day.exe

FAULTING_IP:
win32k!HMUnlockObject+8
929bc55e ff4804          dec     dword ptr [eax+4]

EXCEPTION_RECORD:  ffffffff -- (.exr 0xffffffffffffffff)
ExceptionAddress: 929bc55e (win32k!HMUnlockObject+0x00000008)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 00000001
   Parameter[1]: 41414145
Attempt to write to address 41414145

ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%08lx referenced memory at 0x%08lx. Th

EXCEPTION_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%08lx referenced memory at 0x%08lx

EXCEPTION_PARAMETER1:  00000001

EXCEPTION_PARAMETER2:  41414145

WRITE_ADDRESS:  41414145

FOLLOWUP_IP:
win32k!HMUnlockObject+8
929bc55e ff4804          dec     dword ptr [eax+4]

BUGCHECK_STR:  ACCESS_VIOLATION

DEFAULT_BUCKET_ID:  STRING_DEREFERENCE

CURRENT_IRQL:  0

LAST_CONTROL_TRANSFER:  from 929bc9e0 to 929bc55e

STACK_TEXT:
aae0bc38 929bc9e0 41414141 00010007 00010003 win32k!HMUnlockObject+0x8
aae0bc48 92a2f31c fea22938 00040199 00000000 win32k!HMAssignmentLock+0x45
aae0bca0 92a258a5 fea22938 00000182 0000026c win32k!xxxTrackPopupMenuEx+0x1ce
aae0bd14 8165542a 00040199 00000182 0000026c win32k!NtUserTrackPopupMenuEx+0xc3
aae0bd14 77b864f4 00040199 00000182 0000026c nt!KiFastCallEntry+0x12a
001af83c 763b5f7e 763b4b56 00040199 00000182 ntdll!KiFastSystemCallRet
001af840 763b4b56 00040199 00000182 0000026c USER32!NtUserTrackPopupMenuEx+0xc
001af860 00aa1869 00040199 00000182 0000026c USER32!TrackPopupMenu+0x1b
001af978 00aa1ada 0003001e 001af960 ffffffff 0day!ShowPopupMenu+0x129 [c:\users\rootkit\documen
001afaa8 00aa2290 00a90000 00000000 001f1d59 0day!WinMain+0x15a [c:\users\rootkit\documents\vis
001afb50 00aa201f 001afb64 76201174 7ffdb000 0day!__tmainCRTStartup+0x260 [f:\dd\vctools\crt_bl
001afb58 76201174 7ffdb000 001afba4 77b9b3f5 0day!WinMainCRTStartup+0xf [f:\dd\vctools\crt_bld\
001afb64 77b9b3f5 7ffdb000 77d9310f 00000000 kernel32!BaseThreadInitThunk+0xe
001afba4 77b9b3c8 00aa1181 7ffdb000 00000000 ntdll!__RtlUserThreadStart+0x70
001afbbc 00000000 00aa1181 7ffdb000 00000000 ntdll!_RtlUserThreadStart+0x1b


STACK_COMMAND:  kb

SYMBOL_STACK_INDEX:  0

SYMBOL_NAME:  win32k!HMUnlockObject+8

FOLLOWUP_NAME:  MachineOwner

MODULE_NAME: win32k

IMAGE_NAME:  win32k.sys

DEBUG_FLR_IMAGE_TIMESTAMP:  4a5bc2a2

FAILURE_BUCKET_ID:  ACCESS_VIOLATION_win32k!HMUnlockObject+8
```

```
BUCKET_ID:  ACCESS_VIOLATION_win32k!HMUnlockObject+8

Followup: MachineOwner
---------
```