New issue

Jump to bottom

Open a malformed mng format file, buffer overflow and memory corruption will occur. #516

Open **Aurorainfinity** opened this issue on Jul 9, 2020 · 4 comments

Aurorainfinity commented on Jul 9, 2020

Two issues were found in nomacs in all versions. nomacs does not handle the mng file format very well. When nomacs opens a carefully constructed mng file, nomacs will have a buffer overflow and crash

1. buffer overflow

++
(71c.f7c): 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=00000000 ecx=3ffffc38 edx=045d0000 esi=0425fd80 edi=205d1000
eip=6edc103b esp=03a7f130 ebp=00000000 iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010206
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Users\test\Desktop\nomacs-2.4.6-x86-WinXP\imageformats\qmng4.dll -
qmng4+0x2103b:
6edc103b f3ab rep stos dword ptr es:[edi]
0:011> !exploitable -v

!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: 0x205d1000
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Write Access Violation

Faulting Instruction:6edc103b rep stos dword ptr es:[edi]

Exception Hash (Major/Minor): 0x8c7435c8.0xf37f4977

Hash Usage : Stack Trace:
Major+Minor : qmng4+0x2103b
Instruction Address: 0x000000006edc103b

Description: User Mode Write AV
Short Description: WriteAV
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - User Mode Write AV starting at qmng4+0x000000000002103b (Hash=0x8c7435c8.0xf37f4977)

User mode write access violations that are not near NULL are exploitable.
++

2. memory corruption

(340.62c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=0459e8e1 ebx=00000000 ecx=00000000 edx=00000000 esi=00000000 edi=00000000
eip=6edbd435 esp=03aef3c4 ebp=04592a58 iopl=0 nv up ei ng nz na po cy
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010283
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Users\test\Desktop\nomacs-2.4.6-x86-WinXP\imageformats\qmng4.dll -
qmng4+0x1d435:
6edbd435 880e mov byte ptr [esi],cl ds:0023:00000000=??
0:009> !exploitable -v

!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: 0x0
First Chance Exception Type: STATUS_ACCESS_VIOLATION (0xC0000005)
Exception Sub-Type: Write Access Violation

Faulting Instruction:6edbd435 mov byte ptr [esi],cl

Basic Block:
6edbd435 mov byte ptr [esi],cl
Tainted Input operands: 'cl','esi'
6edbd437 movzx ecx,byte ptr [eax]
6edbd43a mov byte ptr [esi+1],cl
6edbd43d movzx ecx,byte ptr [eax-1]
6edbd441 mov byte ptr [esi+2],cl
6edbd444 movzx ecx,byte ptr [eax+2]
6edbd448 mov byte ptr [esi+3],cl
6edbd44b mov ecx,dword ptr [ebp+248h]
6edbd451 add edx,ecx
6edbd453 add eax,4
6edbd456 lea esi,[esi+ecx*4]
6edbd459 cmp edx,dword ptr [ebp+294h]
6edbd45f jl qmng4+0x1d431 (6edbd431)

Exception Hash (Major/Minor): 0xebb32a1e.0x41bed88a

Hash Usage : Stack Trace:
Major+Minor : qmng4+0x1d435
Major+Minor : qmng4+0x106d
Instruction Address: 0x000000006edbd435

Description: User Mode Write AV near NULL
Short Description: WriteAVNearNull
Exploitability Classification: UNKNOWN
Recommended Bug Title: User Mode Write AV near NULL starting at qmng4+0x000000000001d435 (Hash=0xebb32a1e.0x41bed88a)

User mode write access violations that are near NULL are unknown.

diemmarkus commented on Jul 9, 2020 — Member

thanks for reporting. It appears that this happens with v 2.4.6.
a) Is it reproducible with a more recent version (i.e. 3.14.2)?
b) could you please upload an mng file that causes the exception?

Aurorainfinity commented on Jul 10, 2020 — Author

Yes, I also tested this 3.14.2, and the same problem occurs, both on windows x32 and x64.

crashers.zip

1

diemmarkus commented on Aug 3, 2020 • edited — Member

thanks! I did test it & could reproduce the error. I am having a hard time deciding what to do:
a) ditch mng support

- it is not an official standard
- Qt does not support it anymore

b) keep mng support

- maintaining the current state is easy (but we know of issues like this)

I would be happy about your thoughts

mmuehlenhoff commented on Jun 30

I'd suggest to rather disable/remove support, it's not really relevant (given that GIF and APNG are far more prevalent and natively supported in browsers) and wides the attack surface.

1

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

3 participants