

New issue

Jump to bottom

StepMania 5.0.12 crash report #1890

 Open blbi opened this issue on Sep 10, 2019 · 6 comments

Labels bug crash dependencies

blbi commented on Sep 10, 2019 • edited

Architecture : Window10 (x64)
Crash reason : Access violation (invalid address 0x41107f92=????????)
Crashed thread : ntdll_77570000!RtlpFreeHeap+0x2a2

0:000> g
WARNING: Continuing a non-continuable exception
(4868.6e3c): Access violation - code c0000005 (first chance)
ntdll_77570000!RtlpFreeHeap+0x2a2:
775b5702 8b00 mov eax,dword ptr [eax] ds:002b:41107f92=????????
0:000:x86> dd 41107f92
41107f92 ???????? ???????? ???????? ????????
41107fa2 ???????? ???????? ???????? ????????
41107fb2 ???????? ???????? ???????? ????????

The vulnerability is in newvorbis/lib/codebook.c
Insufficient array bounds checking in the inner for-loop at line 407 for (j=0;jdim;
The patched version of vorbis is already released so we should update the vorbis into latest version

-----Exception analysis-----
KEY_VALUES_STRING: 1

PROCESSES_ANALYSIS: 1

SERVICE_ANALYSIS: 1

STACKHASH_ANALYSIS: 1

TIMELINE_ANALYSIS: 1

Timeline: Ianalyze.Start
Name:
Time: 2019-09-10T06:22:44.558Z
Diff: 558 mSec

Timeline: Dump.Current
Name:
Time: 2019-09-10T06:22:44.0Z
Diff: 0 mSec

Timeline: Process.Start
Name:
Time: 2019-09-10T06:09:54.0Z
Diff: 770000 mSec

Timeline: OS.Boot
Name:
Time: 2019-09-03T02:39:09.0Z
Diff: 618215000 mSec

DUMP_CLASS: 2

DUMP_QUALIFIER: 0

FAULTING_IP:
ntdll_77570000!RtlpFreeHeap+2a2
775b5702 8b00 mov eax,dword ptr [eax]

EXCEPTION_RECORD: (.exr -1)
ExceptionAddress: 775b5702 (ntdll_77570000!RtlpFreeHeap+0x00002a2)
ExceptionCode: c0000005 (Access violation)
ExceptionFlags: 00000000
NumberParameters: 2
Parameter[0]: 00000000
Parameter[1]: 41107f92
Attempt to read from address 41107f92

FAULTING_THREAD: 00006e3c

DEFAULT_BUCKET_ID: INVALID_POINTER_READ

PROCESS_NAME: StepMania.exe

FOLLOWUP_IP:
ntdll_77570000!RtlpFreeHeap+2a2
775b5702 8b00 mov eax,dword ptr [eax]

READ_ADDRESS: 41107f92

ERROR_CODE: (NTSTATUS) 0xc0000005 -

EXCEPTION_CODE: (NTSTATUS) 0xc0000005 -

EXCEPTION_CODE_STR: c0000005

EXCEPTION_PARAMETER1: 00000000

EXCEPTION_PARAMETER2: 41107f92

WATSON_BKT_PROCTAMP: 57ad1b94

WATSON_BKT_PROCV: 5.0.0.0

PROCESS_VER_PRODUCT: StepMania

WATSON_BKT_MODULE: ntdll.dll

WATSON_BKT_MODSTAMP: 1dde673

WATSON_BKT_MODOFFSET: 45702

WATSON_BKT_MODVER: 10.0.17763.475

BUILD_VERSION_STRING: 17763.1.amd64fre.rs5_release.180914-1434

MODLIST_WITH_TSCHKSUM_HASH: 6025c0216d2fbd7954c6688c9d2605f3d339a818

MODLIST_SHA1_HASH: 794baed923caa07f71b528267cd0db95d8a32c54

NTGLOBALFLAG: 0

PROCESS_BAM_CURRENT_THROTTLED: 0

PROCESS_BAM_PREVIOUS_THROTTLED: 0

APPLICATION_VERIFIER_FLAGS: 0

PRODUCT_TYPE: 1

SUITE_MASK: 272

DUMP_TYPE: fe

ANALYSIS_SESSION_HOST: DESKTOP-BLBI

ANALYSIS_SESSION_TIME: 09-10-2019 15:22:44.0558

ANALYSIS_VERSION: 10.0.18362.1 amd64fre

THREAD_ATTRIBUTES:

OS_LOCALE: KOR

BUGCHECK_STR: APPLICATION_FAULT_INVALID_POINTER_READ_ZEROED_STACK

PRIMARY_PROBLEM_CLASS: APPLICATION_FAULT

PROBLEM_CLASSES:

ID: [0n313]
Type: [ACCESS_VIOLATION]
Class: Addendum
Scope: BUCKET_ID
Name: Omit
Data: Omit
PID: [Unspecified]
TID: [0x6e3c]
Frame: [0] : ntdll_77570000!RtlpFreeHeap

ID: [0n285]
Type: [INVALID_POINTER_READ]
Class: Primary
Scope: DEFAULT_BUCKET_ID (Failure Bucket ID prefix)
BUCKET_ID
Name: Add
Data: Omit
PID: [Unspecified]
TID: [0x6e3c]
Frame: [0] : ntdll_77570000!RtlpFreeHeap

ID: [0n158]
Type: [ZEROED_STACK]
Class: Addendum
Scope: BUCKET_ID
Name: Add
Data: Omit
PID: [0x4868]
TID: [0x6e3c]
Frame: [0] : ntdll_77570000!RtlpFreeHeap

LAST_CONTROL_TRANSFER: from 775b50c1 to 775b5702

STACK_TEXT:
004ff988 775b50c1 048a2de0 048a2de8 14771fcc ntdll_77570000!RtlpFreeHeap+0x2a2
004ff9dc 732e0267 005c0000 00000000 048a2de8 ntdll_77570000!RtlFreeHeap+0x201
004ffa20 732ea6fc 00000000 004ffb34 004ffb8 AcLayers!NS_FaultTolerantHeap::FthDelayFreeQueueInsert+0x37a
004ffa58 0172fde8 005c0000 00000000 14ca47e0 AcLayers!NS_FaultTolerantHeap::APIHook_RtlFreeHeap+0x3ac
WARNING: Stack unwind information not available. Following frames may be wrong.
004ffa6c 012f592e 14ca47e0 004ffa8 01668b8b StepMania+0x4cfe8
004ffa78 01668b8b 14ca47e0 00000020 2b8fc256 StepMania+0x9592e
004ffa8 016690c3 004ffb8 004ffb34 004ffb18 StepMania+0x408b8b
004ffb5c 01668ec4 004ffb8 00000000 00000000 StepMania+0x4090c3
004ffb80 0144e57a 004ffb8 004ffa0 004ffb9c StepMania+0x408ec4
004ffbe0 0144dfbf 2b8fc4aa 03fc3c70 00000000 StepMania+0x1ee57a
004ffc04 0157d621 0063ef18 012f53a4 2b8fc4e6 StepMania+0x1edfbf
004ffc48 012fd2fc 2b8fc5a2 00000000 01a056c4 StepMania+0x31d621
004ffd0c 0165e2d6 00000001 006838f0 004ffd20 StepMania+0x9d2fc
004ffd24 01713e09 01260000 00000000 005c3fdd StepMania+0x3fe2d6
004ffd70 74c20419 003df000 74c20400 004ffddc StepMania+0x4b3e09
004ffd80 775d662d 003df000 6fa383e8 00000000 KERNEL32!BaseThreadInitThunk+0x19
004ffddc 775d65fd ffffffff 775f51c7 00000000 ntdll_77570000!_RtlUserThreadStart+0x2f
004ffdec 00000000 01713e7b 003df000 00000000 ntdll_77570000!_RtlUserThreadStart+0x1b

STACK_COMMAND: ~0s ; .cxr ; kb

THREAD_SHA1_HASH_MOD_FUNC: 106168de85fcc28d7817f4926f1b56c7a8e1dbd0

THREAD_SHA1_HASH_MOD_FUNC_OFFSET: 2560686e6e3b73a7ce87d228f2e5569022832851

THREAD_SHA1_HASH_MOD: fc9dfefbcc482ebc09ebcf8406ae8729b26ac0d9

FAULT_INSTR_CODE: 528b008b

SYMBOL_STACK_INDEX: 0

SYMBOL_NAME: ntdll_77570000!RtlpFreeHeap+2a2

FOLLOWUP_NAME: MachineOwner

MODULE_NAME: ntdll_77570000

IMAGE_NAME: ntdll.dll

DEBUG_FLR_IMAGE_TIMESTAMP: 1ddde673

FAILURE_BUCKET_ID: INVALID_POINTER_READ_c0000005_ntdll.dll!RtlpFreeHeap

BUCKET_ID: APPLICATION_FAULT_INVALID_POINTER_READ_ZEROED_STACK_ntdll_77570000!RtlpFreeHeap+2a2

FAILURE_EXCEPTION_CODE: c0000005

FAILURE_IMAGE_NAME: ntdll.dll

BUCKET_ID_IMAGE_STR: ntdll.dll

FAILURE_MODULE_NAME: ntdll_77570000

BUCKET_ID_MODULE_STR: ntdll_77570000

FAILURE_FUNCTION_NAME: RtlpFreeHeap

BUCKET_ID_FUNCTION_STR: RtlpFreeHeap

BUCKET_ID_OFFSET: 2a2

BUCKET_ID_MODTIMESTAMP: 1ddde673

BUCKET_ID_MODCHECKSUM: 1a263d

BUCKET_ID_MODVER_STR: 10.0.17763.475

BUCKET_ID_PREFIX_STR: APPLICATION_FAULT_INVALID_POINTER_READ_ZEROED_STACK_

FAILURE_PROBLEM_CLASS: APPLICATION_FAULT

FAILURE_SYMBOL_NAME: ntdll.dll!RtlpFreeHeap

WATSON_STAGEONE_URL: <http://watson.microsoft.com/StageOne/StepMania.exe/5.0.0.0/57ad1b94/ntdll.dll/10.0.17763.475/1ddde673/c0000005/00045702.htm?Retriage=1>

TARGET_TIME: 2019-09-10T06:22:50.000Z

OSBUILD: 17763

OSSERVICEPACK: 475

SERVICEPACK_NUMBER: 0

OS_REVISION: 0

OSPLATFORM_TYPE: x64

OSNAME: Windows 10

OSEDITION: Windows 10 WinNt SingleUserTS

USER_LCID: 0

OSBUILD_TIMESTAMP: unknown_date

BUILDDATESTR: 180914-1434

BUILDLAB_STR: rs5_release


BUILDOVER_STR: 10.0.17763.1.amd64fre.rs5_release.180914-1434

ANALYSIS_SESSION_ELAPSED_TIME: 1748

ANALYSIS_SOURCE: UM

FAILURE_ID_HASH_STRING: um:invalid_pointer_read_c0000005_ntdll.dll!rtlpfreeheap

FAILURE_ID_HASH: {d7fe17f8-4233-084f-9484-8f5d1b2edc8b}

 **shakesoda** added the **dependencies** label on Sep 10, 2019

shakesoda commented on Sep 10, 2019

Member

can this be easily reproduced? i'm tagging this anyways because we certainly need to update vorbis, but being able to actually tell if it is fixed would be nice.

blbi commented on Sep 11, 2019

Author

yes it is a bug and you can easily reproduce this.
This is the poc, crafted song file.
[Crafted.zip](#)

you can reproduce the crash by editing the action of the song via the *Edit/Share* menu.
the crash occurs when playing a song during editing.

 **shakesoda** added **bug** **crash** labels on Sep 11, 2019

ChronoAndross commented on Feb 25, 2020

Contributor

Hey @blbi I tried reproducing your crash, but it seems like your OGG file is corrupted, making it hard to reproduce the same exact call stack. Oddly enough, I've been getting a number of heap corruptions while playing around in the editor, but they never yield the same call stack when SM crashes. These crashes I'm seeing also seem to be random, and I don't know if that's expected or not (I'm in debug mode, so maybe it is). I'll keep playing around with this in the meantime.

coderjo commented on Feb 25, 2020

Contributor

The stack won't be consistent, due to the way this works, along with things like load address randomization and the like.

The ogg is specially crafted to exploit a bug in vorbis.

 **ChronoAndross** added a commit to ChronoAndross/stepmania that referenced this issue on Mar 14, 2020

 Update Vorbis from 1.3.2 to 1.3.6. Updating to this version addresses... [...](#)

cdf4349

 **ChronoAndross** mentioned this issue on Mar 15, 2020

Update Vorbis from 1.3.2 to 1.3.6. Updating to this version addresses... #1971

 Merged

abergmann commented on Dec 28, 2020

[CVE-2020-20412](#) was assigned to this issue.

 **shakesoda** commented on Dec 28, 2020

Member

oh joyous day, a cve of our very own. i can't deal with it at this moment,
but [#1971](#) looks fine to merge to resolve this (if i saw that pr previously,
i completely forgot about it).
...

Assignees

No one assigned

Labels

bug **crash** **dependencies**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants

