

New issue

[Jump to bottom](#)

fluidsynth crashes when loading malformed sf2 file #808

 Closed

veritas501 opened this issue on Mar 14, 2021 · 11 comments

Labels

bug

Milestone

2.1

veritas501 commented on Mar 14, 2021 · edited

version: master(v.2.1.1), ubuntu18.04(v1.1.9), ubuntu20.04(v.2.1.1),

https://github.com/FluidSynth/fluidsynth/blob/master/src/sfloader/fluid_sffile.c#L1952

It says Gen_SampleId is the last gen, and then set level to 3 and break.

```
else if(genid == Gen_SampleId)
{
    /* sample is last gen */
    level = 3;
    READW(sf, genval.uword);
    ((SFZone *) (p2->data))->instsamp = FLUID_INT_TO_POINTER(genval.uword + 1);
    break; /* break out of generator loop */
}
```

but if a malformed sf2 doesn't contain Gen_SampleId, it will finally goto here:

https://github.com/FluidSynth/fluidsynth/blob/master/src/sfloader/fluid_sffile.c#L2041

```
if(level == 3) // level == 2 because no Gen_SampleId found
{
    SLADVREM(z->gen, p3); /* zone has sample? */
}
else // enter here
{
    /* its a global zone */
    if(!gzone) // not the first time enter here, so gzone == TRUE, skip
    {
        gzone = TRUE;

        /* if global zone is not 1st zone, relocate */
        if(*hz != p2)
        {
            void *save = p2->data;
            FLUID_LOG(FLUID_WARN, "Instrument '%s': Global zone is not first zone",
                ((SFPreset *) (p->data))->name);
            SLADVREM(*hz, p2);
            *hz = fluid_list_prepend(*hz, save);
            continue;
        }
    }
    else // finally enter here and free it, but actually it's gzone. so it will cause an use-after-free later ...
    {
        /* previous global zone exists, discard */
        FLUID_LOG(FLUID_WARN, "Instrument '%s': Discarding invalid global zone",
            ((SFInst *) (p->data))->name);
        *hz = fluid_list_remove(*hz, p2->data);
        delete_zone((SFZone *) fluid_list_get(p2));
    }
}
```

it will be freed again at: https://github.com/FluidSynth/fluidsynth/blob/master/src/sfloader/fluid_sffile.c#L2293

```
entry = zone->gen;

while(entry)
{
    FLUID_FREE(fluid_list_get(entry)); // free at here
    entry = fluid_list_next(entry);
}
```

fluid_synth_sfload() -> fluid_defsfloader_load() -> fluid_defsfont_load() -> fluid_sfclose() -> delete_inst() -> delete_zone()

HERE is an example that trigger this vuln: [vuln.zip](#)

```

veritas@DESKTOP-4VIL7MG:/tmp$ fluidsynth --version
FluidSynth runtime version 2.1.1
Copyright (C) 2000-2020 Peter Hanappe and others.
Distributed under the LGPL license.
SoundFont(R) is a registered trademark of E-mu Systems, Inc.

FluidSynth executable version 2.1.1
Sample type=double
veritas@DESKTOP-4VIL7MG:/tmp$ fluidsynth ./vuln.sf2
FluidSynth runtime version 2.1.1
Copyright (C) 2000-2020 Peter Hanappe and others.
Distributed under the LGPL license.
SoundFont(R) is a registered trademark of E-mu Systems, Inc.

fluidsynth: warning: Instrument 'Contrabassoon      ': Discarding invalid global zone
fluidsynth: error: Instrument 'Contrabassoon      ': Invalid sample reference
fluidsynth: error: Couldn't parse presets from soundfont file
Bus error
veritas@DESKTOP-4VIL7MG:/tmp$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=20.04
DISTRIB_CODENAME=focal
DISTRIB_DESCRIPTION="Ubuntu 20.04.1 LTS"
veritas@DESKTOP-4VIL7MG:/tmp$ |

```

```

veritas@DESKTOP-4VIL7MG:/tmp$ gdb fluidsynth --args fluidsynth ./vuln.sf2
GNU gdb (Ubuntu 9.1-0ubuntu1) 9.1
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from fluidsynth...
(No debugging symbols found in fluidsynth)
(gdb) r
Starting program: /usr/bin/fluidsynth ./vuln.sf2
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[New Thread 0x7ffff67ce700 (LWP 980)]
FluidSynth runtime version 2.1.1
Copyright (C) 2000-2020 Peter Hanappe and others.
Distributed under the LGPL license.
SoundFont(R) is a registered trademark of E-mu Systems, Inc.

fluidsynth: warning: Instrument 'Contrabassoon      ': Discarding invalid global zone
fluidsynth: error: Instrument 'Contrabassoon      ': Invalid sample reference
fluidsynth: error: Couldn't parse presets from soundfont file

Thread 1 "fluidsynth" received signal SIGBUS, Bus error.
0x00007ffff7f06f10 in ?? () from /lib/x86_64-linux-gnu/libfluidsynth.so.2
(gdb) x/i $rip
=> 0x7ffff7f06f10:    mov     0x0(%rbp),%rdi
(gdb) i reg
rax            0x0                0
rbx            0x5555555df000       93824992800768
rcx            0x7ffff7cddb90     140737350851472
rdx            0x5555557be940     93824994765120
rsi            0x1                1
rdi            0x55555555e010       93824992272400
rbp            0x4141414141414141  0x4141414141414141
rsp            0x7fffffff0cc0     0x7fffffffddcc0
r8             0x7                7
r9             0x3e               62
r10            0x7ffff7f3d2b0     140737353339568
r11            0x202              514
r12            0x5555555de2e0       93824992797408
r13            0x5555557be8d0     93824994765008
r14            0x5555557be880     93824994764928
r15            0x5555557be8a0     93824994764960
rip            0x7ffff7f06f10     0x7ffff7f06f10
eflags         0x10206             [ PF IF RF ]
cs             0x33              51
ss             0x2b              43
ds             0x0                0
es             0x0                0
fs             0x0                0
gs             0x0                0
(gdb) |

```

Programs like VLC that use this library are affected by this vulnerability:



utkarsh2102 commented on Apr 24, 2021 • edited

Hello, I wonder if it's also affecting v1.1.11? `static int load_pgen` definition exists in `src/sfloader/fluid_defsfont.c` there which is not way too different than what it is atm. Could somebody confirm if this bug/CVE also applies to v1.1.11?

Thanks!

derselbst commented on Apr 24, 2021

Member

I wonder if it's also affecting v1.1.11?

Pls. refer to the changelog: <https://github.com/FluidSynth/fluidsynth/wiki/ChangeLog#fluidsynth-218>

utkarsh2102 commented on Apr 24, 2021

I wonder if it's also affecting v1.1.11?

Pls. refer to the changelog: <https://github.com/FluidSynth/fluidsynth/wiki/ChangeLog#fluidsynth-218>

Eeks, sorry for not checking earlier. And thanks!

bynt commented on May 5, 2021 • edited

CVE-2021-28421 was assigned for this.

@ajakc:

[GHS-6fcq-pxhc-jxc9](#) mentions CVE-2021-21417 but references [#808](#). Is this a duplicate?

CVE-2021-21417 was assigned by GitHub, maybe automatically.

derselbst commented on May 5, 2021

Member

CVE-2021-21417 is the one I've originally filed via Github security advice. Which actually worked quite smooth, but unfortunately, the CVE stayed "reserved" even after the advice was published on Mar 31. But it seems like it was finally published a few days ago. No clue why it stayed reserved for so long. The best guess I have is that veritas501 hasn't accepted the credit for this CVE. Although according to GH documentation this shouldn't matter... weird.

bynt commented on May 6, 2021 • edited

CVE-2021-21417 is the one I've originally filed via Github security advice.

Thanks for clarifying. I filed an update request for [CVE-2021-28421](#) with Mitre (Duplicate of CVE-2021-21417).

mawe42 commented on May 6, 2021

Member

Hey Martin, funny meeting you here :-)



bynt commented on May 6, 2021

Hey Martin, funny meeting you here :-)

haha, indeed! Fedora brought me here :-)

<https://bodhi.fedoraproject.org/updates/FEDORA-EPEL-2021-f17367545f>

buildroot-auto-update pushed a commit to buildroot/buildroot that referenced this issue on Sep 13, 2021

package/fluidsynth: security bump to version 2.1.9 ...

a995385

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

2.1

Development

No branches or pull requests

6 participants

