New issue

Jump to bottom

in box_code_base.c line 8637 has a heap overflow #1262

Closed 3 tasks **Ch111p** opened this issue on Jul 5, 2019 · 2 comments

Ch111p commented on Jul 5, 2019

Thanks for reporting your issue. Please make sure these boxes are checked before submitting your issue - thank you!

- [ ] I looked for a similar issue and couldn't find any.
- [ ] I tried with the latest version of GPAC. Installers available at http://gpac.io/downloads/gpac-nightly-builds/
- [ ] I give enough information for contributors to reproduce my issue (meaningful title, github labels, platform and compiler, command-line ...). I can share files anonymously with this dropbox: https://www.mediafire.com/filedrop/filedrop_hosted.php?drop=eec9e058a9486fe4e99c33021481d9e1826ca9dbc242a6cfaab0fe95da5e5d95

Detailed guidelines: http://gpac.io/2013/07/16/how-to-file-a-bug-properly/

in box_code_base.c line 8637 has a heap overflow.

```
GF_Err txtc_Read(GF_Box *s, GF_BitStream *bs)
{
        u32 size, i;
        char *str;
        GF_TextConfigBox *ptr = (GF_TextConfigBox*)s;

        size = (u32) ptr->size;
        str = (char *)gf_malloc(sizeof(char)*size);

        i=0;

        while (size) {
                str[i] = gf_bs_read_u8(bs);
                size--;
                if (!str[i])
                        break;
                i++;
        }
        if (i) ptr->config = gf_strdup(str);
        gf_free(str);

        return GF_OK;
}
```

When str is full without '\x00', strdup will make a heap overflow.

jeanlf added a commit that referenced this issue on Jul 5, 2019

`fixed potential crash cf #1262` 3fcf66c

jeanlf commented on Jul 5, 2019 Contributor

now fixed, thanks for the report

jeanlf closed this as completed on Jul 5, 2019

carnil commented on Sep 9, 2021

CVE-2020-19750 was assigned for this issue.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants