#8782 closed defect (fixed)

Opened 2 years ago
Closed 2 years ago

ffmpeg abort when parsing file

Reported by:	lawhack	Owned by:	
Priority:	important	Component:	avformat
Version:	git-master	Keywords:	mm crash abort
Cc:	hackoflpf@163.com	Blocked By:	
Blocking:		Reproduced by developer:	yes
Analyzed by developer:	no		

Description

Summary of the bug:
use afl to fuzz the 4xm fileformat codec,ffmpeg abort when parsing some sample
How to reproduce:

```
% ffmpeg -vcodec 4xm -i sample -f null -
ffmpeg version N-98388-g76a3ee996b Copyright (c) 2000-2020 the FFmpeg developers
built on built with gcc 7 (Ubuntu 7.5.0-3ubuntu1~18.04)
```

Patches should be submitted to the ffmpeg-devel mailing list and not this bug tracker.

Attachments (1)

- sample(126 bytes) - added by lawhack 2 years ago.
  fuzz sample

Change History (3)

by lawhack, 2 years ago

Attachment: *sample*added

fuzz sample

comment:1 by lawhack, 2 years ago

Cc:	hackoflpf@163.com added
Component:	undetermined → ffmpeg
Version:	unspecified → 4.2

comment:2 by Carl Eugen Hoyos, 2 years ago

Component:	ffmpeg → avformat
Keywords:	mm added; bug removed
Priority:	normal → important
Reproduced by developer:	set
Resolution:	→ fixed
Status:	new → closed
Version:	4.2 → git-master

Regression since e045be92cdf5a2851900e8e85b815c29ae6f100a, fixed in ec59dc73f0cc8930bf5dae389cd76d049d537ca7

Note: See TracTickets for help on using tickets.